INTERNATIONAL ASSOCIATION OF JUDGES
2nd STUDY COMMISSION

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 data protection legislation in Italy is governed by 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)*", directly applicable as of 25 May 2018 in all Member States, supplemented by the Italian law on the protection of personal data i.e. d.lgs. 196/2003 and subsequent amendments made, in particular, by Legislative Decree of 18 May 2018 n. 51 implementing EU Directive 2016/680 "*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, and repealing Council Framework Decision 2008/977/JHA*" and Legislative Decree of 10 August 2018 n. 101 which contains a series of provisions for the adaptation of national legislation to the GDPR.

Generally speaking, under the General Data Protection Regulation (Art. 24 et seq.), the data controller must implement appropriate technical and organisational measures to demonstrably ensure that data processing is carried out in accordance with the European regulation, taking into account the nature, scope, context and purpose of the data processing.

Regarding the designation of the data protection officer, Article 37 of the General Data Protection Regulation states in paragraph 1 that: "*the controller and the processor shall designate a data protection officer in any case where: a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity*". Whereas, paragraph 1 of Article 2-sexiesdecies of Legislative Decree 196/2003 provides at national level that "*the data protection officer shall be designated, in accordance with the provisions of Section 4 of Chapter IV of the Regulation, also in relation to the processing of personal data carried out by judicial authorities in the performance of their duties*".

The national rule must be considered as prevailing since it has an additional protective character compared to the European regulation.

This being the case, therefore, Italian judicial offices may be considered data controllers and data processors in all the situations indicated in the question:

a. when they perform their judicial functions, because they manage and process personal data of the parties involved in the proceedings. However, the legislation takes into account the specificity of the judicial purpose, in fact the protection of privacy cannot be an obstacle to the exercise of the judicial function;

b. for purposes connected with the administration of justice, such as the publication of court judgments and decisions, the drawing up and publication of lists or calendars of proceedings or hearings in proceedings

c. for purposes related to the efficient and operational management of judicial offices and for statistical purposes, as judicial offices may process personal data in order to manage their activities efficiently, e.g. for organisational, administrative and statistical purposes relating to proceedings.

With regard to the ownership of the data processing, it should be specified that, in Circular No. 21611.U of 27.6.2018, the Ministry of Justice specified that all processed data relating to the administrative activity carried out in the Judicial Offices must fall under the ownership of the Ministry, while the ownership of the processing of judicial data must fall to the Judicial Offices. In the context of the activity of judicial offices, the distinction between administrative and judicial data became necessary precisely to identify the different data controllers on the basis of the activity, administrative or judicial, carried out and the formal recognition of the autonomy of the judicial function and, therefore, its protection.

However, it should also be pointed out that with the entry into force of the European Regulation, the expression "*judicial data*" is no longer present in the national legislation and has been replaced by the expression "*data relating to criminal convictions and offences*" (Art. 10 Reg. 2016/679) which, however, does not exhaust the set of data processed in judicial proceedings and in the administrative activities connected to them. For this reason, the broader definition of "*judicial data*" used at national level by the Ministry of Justice should be interpreted as including all personal data processed in civil (and criminal too) judicial activities. In this regard, about the limitations of the data subject's rights for reasons of justice, Article 2-duodecies, paragraph 4, of Legislative Decree 196/2003, as amended by Legislative Decree 101/2018, expressly provides that "*the processing of personal data related to the judicial handling of business and disputes* (...) *shall be understood as being carried out for reasons of justice*": the reference is to the conduct of civil and voluntary jurisdiction proceedings in the context of which the data controller of the relevant data is the Judicial Office. Therefore, it can be said that the Judicial Office is the data controller in relation to all personal data in contentious and voluntary civil proceedings (as well as in criminal proceedings).

The judicial office as data protection officer has tasks not only of an advisory nature, but also of monitoring the compliance of processing by judicial bodies with privacy regulations and of cooperation with the "Garante della privacy" (i.e. the Italian Data Protection Supervisor). The legislation also requires the keeping of processing registers, which map processing operations and must be kept in the event of checks by the "Garante". Judicial privacy requires compliance with adequate security measures and the drafting of a privacy impact assessment in the event of high risks to personal privacy. In addition, in the event of a data security breach, the judicial authority must also report the incident to the privacy guarantor.

It should be noted that, in order to ensure autonomy and independence in the exercise of judicial functions, the "Garante della privacy" is not competent to exercise control over the data processing performed by the judicial authority in the exercise of the judicial and prosecutorial functions of the public prosecutor.

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?

In the Italian jurisdiction, data subjects (such as litigants, witnesses or persons whose interests may be affected by the dispute) have the right to receive information about the processing of their personal data by or on behalf of judicial offices. This right is enshrined in the General Data Protection Regulation (GDPR) and further supported by Italian data protection legislation.

The information notice is a communication, provided free of charge, by which the purposes and methods of the processing operations carried out by the data controller are brought to the attention of the citizen, even before he/she becomes a data subject. It constitutes an obligation of data controllers

and it is preparatory to the legitimacy of the processing itself. The right to receive information during processing is governed by Article 15 Reg. 2016/679, while the contents of the information notice are listed exhaustively in Articles 13(1) and 14(1) of the same European regulation. Also taking into account the regulations in force, what is indicated by the "Garante della privacy" (i.e. the Italian Data Protection Supervisor) and what is published on the website of the Ministry of Justice, the information notice to be rendered by the judicial offices must contain: the regulatory sources on privacy; the identity and contact details of the data controller of the Data Protection Officer (DPO); the legal basis and the purposes of the processing (already identified at regulatory level); the processing methods; the rights of the data subjects in relation to access to their data, cancellation, restriction of processing, opposition to processing, right of complaint; information on cookies and browsing data; the date on which the notice is updated. Data subjects also have the right to know the duration of data retention and the existence of other rights, such as the right to rectification, erasure or restriction of processing.

Judicial offices, as data controllers of judicial data, are obliged to provide this information to data subjects and must ensure that individuals are informed about the processing of their personal data, especially when it directly affects their rights and interests in the context of litigation proceedings.

In this regard, it should be noted that recital 58 of the European Regulation provides 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. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand*".

While it is true that data subjects have the rights of access to data, of deletion and rectification of data and of opposition to processing, it is also true that these rights must take into account the needs of investigations and the performance of other judicial activities and must be exercised in accordance with the rules of the Code of Civil Procedure.

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?

In the Italian jurisdiction, a data subject whose personal data is published in a judicial document, such as a judgment, has the right to request the rectification of personal data deemed inaccurate or improperly disclosed.

According to the European Union's General Data Protection Regulation (GDPR), data subjects have the right to have their personal data rectified in the event of inaccurate or incomplete data. This right also applies to personal data published in a judicial document.

If personal data is deemed inaccurate or improperly disclosed in a judicial document, the data subject may request the rectification or deletion of such data, based on the provisions of the GDPR and Italian data protection legislation.

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?

In the Italian jurisdiction, the protection of personal data contained in judicial orders must be balanced with the general principle of publicity of judicial orders themselves. In this regard, at the national level, Articles 51 and 52 of Legislative Decree 196/2003 regulate "*legal information technology*" (although one should more correctly speak of judicial information technology).

Article 51(2) establishes that judgments and other judicial decisions "*are also made accessible through the information system and the institutional website of the same authority on the Internet, observing the precautions provided for*" Article 52 below, such as the hypotheses of mandatory (provided for *ex lege*) or possible (at the request of the party or ordered *ex officio* by the judge) obscuration of personal data. The possibility of access to judgments and other decisions of judicial authorities of any order and degree is not here circumscribed to persons with a specific interest, but extended without any particular limitations, in line with the principle of publicity of the judgment and its final act. More in detail, if there are legitimate reasons, the interested party (which does not necessarily coincide with the party to the judgment) may request, before the finalisation of the relevant level of judgment, that an annotation be made on the original of the judgment or order aimed at precluding, precisely in the event of the reproduction of the judgment or order in any form, the indication of the personal details and other identifying data of the same interested party contained in the judgment or order. The judge may also order, *ex officio*, that certain personal data be rendered anonymous in order to protect the rights or dignity of the persons concerned, as, for example, in cases where sensitive data are indicated in the judgment or order. In other cases, the anonymisation of personal data is provided for directly by law, such as in the case of: data capable of identifying persons under the age of 18; data relating to victims of sexual offences; data of the parties to proceedings concerning the family or status of persons.

Apart from the hypotheses in which obscuration of personal data is required (Article 52(5) provides that "*whoever disseminates judgments or other judicial measures of the judicial authorities of any order and degree is obliged to omit, in any case,* (...) *personal details, other identifying data or other data also relating to third parties from which the identity of minors or of the parties in proceedings concerning family relationships and personal status may be inferred even indirectly*"), Article 52(7) allows "*the dissemination in any form of the content, even in full, of judgments and other judicial decisions*".

Ultimately, the provisions of arts. 51 and 52 of Legislative Decree 196/2003 enshrine the principle of full publication (also online) of judgments as a general rule, subject to the exceptions inherent in any obscuration (ordered at the request of a party or *ex officio*) or mandatory.

With regard to the accessibility of court orders, it should be noted that Article 744 of the Code of Civil Procedure indicates the duty of the clerk of the court to send to anyone who so requests (and not only to anyone who has an interest) "*copies and extracts of court documents held by them, under penalty of damages and costs*", except in certain cases provided for by law.

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?

In national law, complaints relating to alleged violations of data subjects' rights by judicial offices can be lodged through recourse to the judicial authority or to the "Garante per la protezione dei dati personali" (i.e. the Italian Data Protection Supervisor).

Article 140-bis of Legislative Decree 196/2003 provides that "*if the data subject considers that his or her rights under data protection law have been infringed, he or she may lodge a complaint with the Garante or appeal to the judicial authority*". The provision in question establishes the principle of alternativeness of the forms of administrative and judicial protection, and in this regard provides that an appeal to the "Garante" cannot be lodged if a judicial authority has already been

seized for the same object and between the same parties, and that the lodging of a complaint to the "Garante" renders a further application before the judicial authority between the same parties and for the same object inadmissible. Ultimately, the principle of alternativeness concerns only those applications having an identical object, i.e. those which, if pending at the same time before more than one court, may be subject to the procedural institutes of lis pendens or of the continence of cases. Since the "Garante" may indicate concrete modalities for the cessation of unlawful data processing, it must be assumed that these are claims that require preventive, injunction or conforming actions. On the other hand, a claim for compensation for pecuniary or non-pecuniary damage resulting from a breach of data protection legislation can only be brought before the judicial authority, since the "Garante" cannot decide on compensation claims.

As regards the supervision of data processing operations by judicial offices when they act in the exercise of their judicial function, there is no specific person or body, there would be a risk of jeopardising the fundamental principle of independence of the judiciary. In any case, the Italian Data Protection Authority (the "Garante della privacy") can monitor and enforce data protection legislation in all sectors, including the judiciary, without interfering with the autonomy and independence of the judiciary.

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

In the Italian experience, data protection rules do not have a negative impact on the independence of the judiciary in the exercise of judicial functions.

These rules impose obligations and responsibilities on data controllers, including judicial offices, but are implemented with the aim of striking a balance between protecting the privacy of individuals and ensuring transparency and accountability in data processing activities, without their application interfering with the autonomy and independence of the judiciary.

Moreover, Article 23(1)(f) of the GDPR expressly provides the possibility for Member States to restrict by legislative measures the scope of the obligations and rights set out in the Regulation in order to safeguard the independence of the judiciary and judicial proceedings (the provision states that "*the law of the Union or of the Member State to which the controller or processor is subject may restrict, by means of legislative measures, the scope of the obligations and rights referred to in Articles 12 to 22 and 34, as well as in Article 5, in so far as the provisions contained therein correspond to the rights and obligations referred to in Articles 12 to 22, where such a limitation respects the essence of fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:* (...) f*) the safeguarding of the independence of the judiciary and judicial proceedings*").

Taking advantage of this exemption, the national legislator introduced Article 2 duodecies of Legislative Decree 196/2003, which regulates the limitations on the rights of data subjects for reasons of justice and provides that "*in relation to the processing of personal data carried out for reasons of justice within the framework of proceedings before judicial offices of every order and degree as well as before the Superior Council of the Magistracy and the other self-governing bodies of the special magistracies or at the Ministry of Justice, the rights and obligations referred to in Articles 12 to 22 and 34 of the Regulation shall be governed within the limits and in the manner laid down by the provisions of the law or of the Regulation governing such proceedings, in compliance with the provisions of Article 23(2) of the Regulation*".

Finally, as already pointed out (see above reply to question 1), it should be noted that precisely in order to guarantee autonomy and independence in the exercise of judicial functions, the "Garante della privacy" (i.e. the Italian Data Protection Authority) is not competent to exercise control over the data processing operations carried out by the judicial authority in the exercise of the judicial and prosecutorial functions of the public prosecutor.