

**INTERNATIONAL ASSOCIATION OF JUDGES**  
**2 nd STUDY COMMISSION Answers from Greece**

**Introduction**

The right to the protection of personal data is a fundamental right compliance with which is an important objective for the European Union. It is enshrined in the Charter of Fundamental Rights of the European Union ('the Charter') which provides, in Article 8. That fundamental right is, moreover, closely connected with the right to respect for private and family life enshrined in Article 7 of the Charter. The right to the protection of personal data is also laid down in Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), which succeeded Article 286 EC in that respect. As regards secondary legislation, the European Community has, since the mid-1990s, developed a range of instruments to ensure the protection of personal data. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1 adopted on the basis of Article 100a EC, is the Union's principal legal instrument in this area. It lays down the general rules on the lawfulness of the processing of such data and the rights of data subjects and provides in particular for the establishment of independent supervisory authorities in Member States.

Directive 2002/58/EC subsequently supplemented Directive 95/46 by harmonising the provisions of Member States' legislation on the protection of the right to privacy, notably with respect to the processing of personal data in the electronic communications sector. It should be noted that the Union legislature is considering a review of that directive. In that regard, on 10 January 2017, the Commission put forward a proposition to replace that directive by a regulation relating to privacy and electronic communications. In addition, in the area of freedom, security and justice (ex Articles 30 and 31 TEU), Framework Decision 2008/977/JHA 5 regulates (until May 2018) the protection of personal data in the areas of judicial cooperation in criminal matters and police cooperation. In 2016, the European Union reformed the overall legal framework in this area. To that end, it adopted Regulation (EU) 2016/679 on data protection ('the GDPR'), which repeals Directive 95/46 and has been applicable from 25 May 2018, and Directive (EU) 2016/680 on the protection of such data in

criminal matters, which repeals Framework Decision 2008/977/JHA and was required to be transposed by Member States by 6 May 2018. Last, in the context of the processing of personal data by the EU institutions and bodies, Regulation (EC) No 45/2001 ensured, first of all, the protection of such data.<sup>8</sup> In particular, the regulation enabled the European Data Protection Supervisor to be established in 2004. In 2018, the European Union adopted a new legal framework in this area, in particular through the adoption of Regulation (EU) 2018/1725, which repeals Regulation (EC) No 45/2001 and Decision No 1247/2002/EC<sup>10</sup> and is applicable from 11 December 2018. In the interest of a coherent approach to personal data protection throughout the Union, that new regulation aims to align as far as possible the rules in this area with the regime established by the GDPR.

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

**a. When performing its juridical functions?**

In Greek jurisdiction, each court (or formation of the court) is considered as controller. In particular, civil courts, including all Civil Divisions of the Supreme Court (Areios Pagos), and the administrative courts, including the Council of State and the Court of Auditors are considered as controllers within the meaning of Article 4 No. 7 GDPR [(EU) Regulation 2016/679]. Also, criminal courts, including the Criminal Chambers of the Supreme Court, misdemeanour courts, investigating judges and criminal judicial councils, are considered as controllers within the meaning of Article 44 para. g) of Law 4624/2019 (A' 137), according to which "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, and repealing Council Framework Decision 2008/977/JHA" was transposed into the Greek national law.

**b. For purposes connected with the administration of justice, including the publication of a judgement or court decision, or a list or schedule of proceedings or of hearing in proceedings?**

The scope of both the above GDPR and the aforementioned Law 4624/2019 falls, accordingly, any processing of personal data carried out by the courts in the exercise of their judicial function, whether it concerns the administration of justice or the publication of court decisions (to the extent that these court decisions have not been anonymized). In particular, the tables and exhibits of civil and criminal courts and criminal proceedings in general (either in their handwritten or digital form) are anonymized and therefore do not fall within the scope of either the above GDPR or the aforementioned law.

**c. For purposes connected with the efficient management and operation of the courts and for statistical purposes?**

The same applies to the efficient administration and functioning of the courts and for statistical purposes (JustStat). That is, when personal data is not anonymized, they fall within the scope of the GDPR and Law 4624/2019 (=regarding the adoption of measures for the implementation of the GDPR).

**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 party to the civil proceedings may exercise all the rights of information deriving from the provisions of Chapter III of the GDPR (in particular Articles 12, 13, 14 and 15). On the other hand, a third party, non-party, or witness, who has no legal interest in the outcome of the proceedings or where the processing of personal data does not affect him/her is not allowed to exercise the above information rights.

**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 party to the civil proceedings may exercise all the rights of information deriving from the provisions of Chapter III of the GDPR (in particular Articles 12, 13, 14 and 15). On the other hand, a third party, non-party, or witness, who has no legal interest in the outcome of the proceedings or where the processing of personal data does not

affect him/her is not allowed to exercise the above information rights.

**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?**

-As a rule, court decisions or court acts or orders, etc. , which are to be made public to an indefinite number of persons after publication are anonymised, just as the CJEU has accepted and applies in its published decisions. The same applies, as mentioned above, when drawing up court tables and exhibits.

**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?**

From the combined application of Article 55 para. 3 GDPR and Art. 10 para. 5 of Law 4624/2019 "The Authority is not competent to control processing of personal data carried out by judicial and prosecutorial authorities in the context of their judicial function and judicial duties..." it follows that the Greek "Personal Data Protection Authority" cannot control the processing of personal data carried out by judicial or prosecuting authorities in the exercise of their judicial function. However, when personal data breaches take place not in the exercise of the judicial and prosecuting authorities, then the data subject may complain to the independent Greek "Personal Data Protection Authority" (Articles 9, 13, 15 and 58 of Law 4624/2019).

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

From the combined application of Article 55 para. 3 GDPR and Art. 10 para. 5 of Law 4624/2019 "The Authority is not competent to control processing of personal data carried out by judicial and prosecutorial authorities in the context of their judicial function and judicial duties..." it follows that the Greek "Personal Data Protection Authority" cannot control the processing of personal data carried out by judicial or

prosecuting authorities in the exercise of their judicial function. However, when personal data breaches take place not in the exercise of the judicial and prosecuting authorities, then the data subject may complain to the independent Greek "Personal Data Protection Authority" (Articles 9, 13, 15 and 58 of Law 4624/2019).