CHIOMENTI

Key News

IP, TMT and Data Protection Department
September 2020

Summary

I Guidelines on the concepts of controller and processor in the GDPR

Since the entry into application of the General Data Protection Regulation (GDPR) and in light of the recent rulings of the Court of Justice of the European Union (CJEU), questions have been raised as to what effect the new regulation brought to the concepts of data controller and data processor, particularly regarding the concept of joint controllership (Article 26 GDPR), as well as the obligations for processors (as mainly referred to in Article 28 GDPR).

For these reasons, on September 2, 2020, the European Data Protection Board (EDPB) issued the "Guidelines 07/2020 on the concepts of controller and processor in the GDPR", currently subject to public consultation.

There is no doubt that the concepts of controller and processor have not changed with the GDPR, compared to the Directive 95/46/EC. The EDPB aims to specify that these concepts

are “functional concepts” (i.e., the allocation of responsibilities must be carried out according to the actual roles of the parties) and “autonomous concepts” (i.e., they should be interpreted mainly according to EU data protection law).

With particular regard to the concept od data controller, the EDPB points out that in many cases, the terms of a contract can help identify the controller, although they are not decisive in all circumstances. In addition, some more practical aspects of implementation relating to a given data processing (“non-essential means”) can be left to the processor, without this affecting the ownership of the processing. At the same time, it is not necessary that the controller actually has access to the data that is being processed to be qualified as a controller.

As far as the joint controllership is concerned, the EDPB clarify that an important criterion is that the processing would not be possible without both parties’ participation, in the sense that the processing by each party is inseparable – i.e., inextricably linked. The joint participation needs to include both the determination of purposes and the determination of means.

The EDPB moreover specifies that not every service provider that processes personal data in the course of delivering a service automatically acts as a “processor” within the meaning of the GDPR. The role of a processor does not stem from the nature of an entity that is processing data but from its concrete activities in a specific context.

The end date for providing feedback in the context of the public consultation is October 19, 2020.

Here is the *link* to download the Guidelines.

II EDPB GUIDELINES ON SOCIAL MEDIA TARGETING

The European Data Protection Committee (EDPB) has adopted and publicly consulted the Guidelines on targeting of social media users (Guidelines 8/2020).

Targeting activities are an integral part of social media business models as they are aimed at ensuring that the message conveyed by a specific subject (the target) reaches a specific user (or group of users). This is based on the assumption that the greater the consistency of the message with the user's interests, the greater the conversion rate (*i.e.*, the percentage of users who have performed a certain action, the goal of a campaign) and therefore the effectiveness of the campaign is greater.

The targeting operations have become more and more sophisticated, being the result of the combination and analysis of multiple information coming from the most varied sources. The protection of personal data has sometimes presented problems with regards to the transparency of the processing, since it is not clear - among other things - who the owner was and who the campaign originated from. These shortcomings, especially in some specific contexts (*e.g.*, electoral campaigns), take on particular relevance since social media targeting activities may potentially interfere with the formation of citizens' decisions and thus with democratic processes.

The main goal of the Guidelines is, therefore, to identify the various types of targeting, clarify the roles and responsibilities of the platforms and targets (also in terms of joint ownership), define the contractual provisions that govern the agreements, map the risks for the data subjects individual freedoms and identify measures to ensure the protection of personal data and the particular categories of personal data involved.

Interested parties may submit any comments by 19 October 2020.

Here is the *link* where you can view the text of the Guidelines.

III EDPB GUIDELINES ON THE INTERPLAY OF THE SECOND PAYMENT SERVICES DIRECTIVE AND THE GDPR

On 17 July 2020, the EDPB adopted the Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR. The Guidelines clarify under which terms the GDPR interacts with the Second Directive on Payment Services (2015/2366/EU – s.c. PSD2), which was transposed in Italy with Legislative Decree 218/2017 and entered into force in January 2018. The PSD2 aims to promote the development of retail payments by strengthening the protection of payment service users, supporting innovation and increasing the level of security of electronic payment services.

Taking up what the EDPB already reported in July 2018 in a first letter of clarification, the Guidelines - which the EDPB has placed in public consultation, concluded on 16 September 2020 - aim to provide further guidance on data protection aspects in the context of PSD2, by focusing mainly on the processing of personal data by AISPs (Account Information Service Providers) and PISPs (Payment Initiation Service Providers). The Guidelines address the conditions for granting access to payment account information by Account Servicing Payment Service Providers (ASPSPs) and for the processing of personal data by PISPs and AISPs, including the requirements and guarantees in relation to the processing by PISPs and AISPs for purposes other than the initial purposes for which the data was collected, in particular when it was collected in the context of providing the information service.

Furthermore, the Guideline also deal with the different notions of explicit consent under the PSD2 and the GDPR, the processing of "silent party data" (i.e. personal data concerning the data subject who is not the user of a specific payment service provider, processed for the execution of a contract between the provider and the payment service user), the processing of particular categories of personal data by PISPs and AISPs, the application of the main data protection principles established by GDPR, including the principles of minimization, transparency, accountability and security measures.

Here is the *link* where you can view the text of the Guidelines.

IV ABUSIVE USE OF DATABASES IN THE CONTEXT OF MARKETING ACTIVITIES

The Italian Supreme Court, with judgment No. 18288/2020 filed on 3 September 2020, rejected the main appeal lodged by a company (Company) – ordered – in the first instance proceedings - to pay a fine of Euro 340,000 for abusive use of databases in the context of commercial and telemarketing activities (violation of Articles 162, paragraph 2-bis, 164 and 164-bis paragraph 2 of Legislative Decree No. 196/2003 – Italian Privacy Code) - and grants the cross appeal presented by Italian Supervisory Authority (*Autorità Garante per la protezione dei dati personali*), referring the case back to the Court of Rome.

The Company proposed:

(i) *Two issues of constitutional legitimacy:*

a. Breach of Article 77 of the Italian Constitution because the disputed rules (Articles 162, paragraph 2-bis and 164-bis) were introduced with Decree-Law No. 207/2008 in the absence of the requirements of necessity and urgency. In the case at stake, the Supreme Court considers the issue manifestly unfounded as the conditions for the applicability of Article 77 of the Italian Constitution are not met, namely the legitimacy of the use of the urgency decree is limited only to cases of "*obvious lack of conditions" or of "Evident unreasonableness and arbitrariness of the relative evaluation*". The Supreme Court, similarly to what argued by the General Procurator, considers that "*increased sanctions concerning the regulation of the processing of personal data in contexts of abuse of databases for the purposes of commercial promotion and telemarketing appeared to be necessary, precisely because of the oligopoly of some companies in the collection and processing, without the consent of the data subjects, of data acquired in public archives or in the public domain*".

b. Article 164-*bis* of the Italian Privacy Code is unconstitutional for violation of the *ne bis in idem* principle, enshrined in Protocol 7 of the European Convention on Human Rights and Article 50 of the Charter of Fundamental Rights of the European Union. The Company considers that - through the provisions referred to in Article 164-*bis* - it was condemned twice for the same matter (namely, the lack of privacy notice pursuant to Article 161 and the processing without consent pursuant to Article 162, paragraph 2-*bis*).

   The Supreme Court, taking up what was stated in first instance, considers that the complaint is manifestly inadmissible due to lack of relevance. Essentially, the Supreme Court absorbed the sanction referred to in Article 162, paragraph 2-*bis* in the most serious case set forth in Article 164-*bis*. Moreover, the complaint is not admissible because it is not based on the "*ne bis in idem*" criteria developed by the European Court: "*in the case at stake there is no trace of the application of criminal sanctions nor of the parallel initiation of criminal proceedings for the same facts*".

(ii) *Three grounds for appeal:*

a. Breach and / or false application of Article 1 of Law No. 689/1981 and Articles 13, paragraph 4 and 161 of Italian Privacy Code. The Supreme Court deems this ground of appeal unfounded and - similarly to the findings of the Court of First

Instance - clarifies that the offense committed is continuous. The conduct, in fact, "*continued until the date indicated in the provision of the Authority, since the company could stop such conduct at any time*".

b. Breach and / or false application of Article 14 of Law No. 689/1981 in relation, respectively, to the Articles 360 n. 3 and 5 of the Italian Civil Code. The Supreme Court considers this ground of appeal unfounded as "*in the matter of administrative offenses referred to in the privacy code, the dies a quo for the calculation of the ninety-days deadline for the notification of the complaint report starts from the assessment*" which, in the case at stake, took place in March 2010 only.

c. Breach and / or false application of Article 28 of Law 689/1981 and Articles 13, paragraph 4 and 161 of the Italian Privacy Code. Essentially, the Company invokes the statute of limitation of the offenses as a consequence of the instantaneous nature of the case. However, the Supreme Court finds the ground unfounded for the same reasons set out in the above-extended par. (ii), lett. a).

On the other hand, the Supervisory Authority lodged a cross appeal based on a single ground of appeal with which contested the violation and false application of Articles 164-*bis*, 161 and 162 of the Italian Privacy Code. In the opinion of the Supervisory Authority, the Court of First Instance found that the joint application of the aforementioned rules constituted a violation of the *ne bis in idem* principle. The Supreme Court, therefore, considers the reason adopted by the Supervisory Authority well-grounded and granted it.

V LAWFULNESS OF AN INTERNAL COMMUNICATION ON A WELL-KNOWN DISEASE AFFECTING A POLYCLINIC EMPLOYEE

The Italian Supreme Court (*Corte Suprema di Cassazione*) with judgement No. 16560/2020 filed on 31 July 2020, sentenced the inadmissibility of the appeal lodged by a nurse, employed at a polyclinic in Rome (*Policlinico Umberto I di Roma*), against a judgement issued by the Court of Rome which, in turn, had rejected the appeal against the unfavorable decision of the Italian Supervisory Authority (*Autorità Garante per la protezione dei dati personali*).

The nurse had lodged a complaint with the Supervisory Authority alleging an unlawful dissemination, committed by his employer, of certain personal data concerning his health. Such unlawful dissemination allegedly occurred in the form of a communication sent by the head-nurse of the related unit to certain staff members of the polyclinic (i.e. the director of the nursery office, the coordinator of the psychiatry department and the contact person for external areas). Most notably, the communication at issue would have referred to the opportunity for the nurse to undergo an extraordinary medical examination before the competent doctor of the occupational medicine service, pursuant to Legislative Decree No. 81/2008, due to "hyperglycemic issues" as well as a periodic "plasmapheresis treatment under outpatient procedure".

The complaints raised by the nurse have not been upheld by the Supervisory Authority and, subsequently, by the Court of Rome on the grounds of the news about his disease having been

already disclosed – by the nurse himself – in the working environment. In autonomously displaying his health data, the data subject *de facto* gave his implicit consent to its processing, more broadly, thereby fading the need to protect his privacy. At the same time, the communication sent by the head-nurse of the related unit would not result in a "dissemination" of personal data, rather being an internal reporting directed at the head-nurse's hierarchical superiors. Furthermore, such communication was deemed aiming at protecting the health of the nurse as well as that of third parties – including the users of the polyclinic services – in the framework of Article 5 of Law No. 300/1970 so-called "Workers' Statute" (*Statuto dei Lavoratori*).

Following reassertion about reasons supporting the appeal overstepping the limits of the proceedings before the Supreme Court (as findings of fact on processing of personal data would lead to interpretation of evidence – *ex aliis* Supreme Court judgements No. 18443/2013, No. 2196/2016, No. 19423/2017), the latter highlighted that the Court of Rome has substantially motivated the lawfulness of the communication at issue which – based on the abovementioned assumptions – resulted as not exceeding, rather being dutiful, with respect to the purposes of calling on the nurse to undergo medical examinations, also in his best interest.

VI UNLAWFUL PUBLISHING OF AN EMPLOYEE'S DATA ON THE OFFICIAL BULLETIN BOARD OF THE MUNICIPALITY

With judgment No. 18292/2020 filed on 3 September 2020, the Italian Supreme Court (*Corte Suprema di Cassazione*) dismissed, as inadmissible and ill-founded, the appeal filed by the municipality of Santa Ninfa (TP) against judgment No. 308/2016 of the Court of Sciacca. As the latter judgement had, in turn, rejected the opposition of the municipality against injunction No. 193 of 26 March 2015, of the Italian Supervisory Authority (*Autorità Garante per la protezione dei dati personali*), the dismissal decision of the Supreme Court resulted in the monetary fine of Euro 4,000 imposed against the municipality being upheld.

The case stemmed from the publication of certain municipal resolutions regarding an employee of the municipality of Santa Ninfa on its online official bulletin board. The resolutions, which have been available on the municipality's website for a period longer than one year, displayed the name and surname of the employee, the existence of a judicial dispute between the latter and the municipal administration (information required to justify the appointment of a lawyer with a consequent commitment of expenditure for the municipality), as well as further personal data relating to the employee, such as her family status, the circumstance that she lived alone and that she made a request (denied) to pay the amounts due to the municipality in installments.

The conduct of the municipality had been sanctioned by the Supervisory Authority as it violated former Article 19, paragraph 3, of Legislative Decree No. 196/2003 (Italian Privacy Code) which was applicable *ratione tempori* to the case at hand. Indeed, pursuant to former Article 19, Paragraph 3: "*Communication by a public body to private individuals or economic public bodies and dissemination by a public body is allowed only when they are set forth by a provision of law or regulation*". Most notably, the Supervisory Authority found that the conduct of the municipality was in breach of the above provision since, although the employee's personal data had been lawfully published on the online official bulletin board pursuant to Article 124 of Legislative Decree No. 267/2000 (Law on Local Authorities), the dissemination thereof - and,

in particular, of the data relating to the employee's private life - through the publication on the website of the municipality had extended for a period longer than the required period set forth by the aforementioned Article 124 (*i.e.*, fifteen days).

In dismissing the municipality's grounds of appeal, the Supreme Court clarified, *inter alia*, that the injunction of the Supervisory Authority did not conflict with the requirements of transparency which are inherent to the activity of public bodies, as the information relating to the employee's private life did not relate to the organizational structure of the municipal offices. Furthermore, the Supreme Court took stance on the municipality's contention that the latter cannot be considered liable for failure to remove the personal data, since an external consultant was entrusted by the municipality with the maintenance of the website in accordance with applicable laws, on its behalf. The above contention was rejected by the Supreme Court on the basis of former Article 28 of the Italian Privacy Code, whereby the data controller shall be the legal person and not the representatives or the directors thereof, thus entailing a derogation of the principle of personal liability provided for administrative sanctions.

Contacts

Gilberto Nava
Partner – Chiomenti
IP, TMT, Data Protection
T. +39.06.46622.719
gilberto.nava@chiomenti.net

Giulio Vecchi
Counsel – Chiomenti
IP, TMT, Data Protection
T. +39.0272157658
giulio.vecchi@chiomenti.net