Newsletter JUNE 2021

THE NEW SCCs FOR INTERNATIONAL DATA TRANSFER; PRIVACY DAMAGES COMPENSATED ONLY IF SERIOUS; ONE SHOP STOP DOES NOT PREVENT SUPERVISORY AUTHORITIES FROM EXERCISING THEIR POWERS

The commission of the European Union approves new sets of standard contractual clauses

On the 4th of June 2021, the EU Commission approved two new sets of standard contractual clauses concerning the application of the Regulation (EU) 2016/679 (General Data Protection Regulation or "**GDPR**") (and, *mutatis mutandis,* also of the Regulation (EU) 2018/1725, which, however, will not be discussed here). In particular, two distinct legal instruments have been adopted based on different provisions of the GDPR:

(i) The clauses governing the relationship between controllers and processors, pursuant to Article 28(7) GDPR, (Decision 2021/915/EU); and

(ii) The clauses providing adequate safeguards for transfers outside the European Union (Decision 2021/914/EU), pursuant to Article 46(2)(c) GDPR.

These new sets of standard clauses were published in the Official Journal of the European Union on the 7th of June 2021 (L199) and will officially enter into force on the 27th of June 2021, *i.e.* on the twentieth day after publication.

1. The new standard clauses for transfers: things to know

1.1 The standard clauses for data transfers. The update of these clauses is long-overdue, as the last clauses in force were adopted more than 11 years ago.

1.2 The main changes. In their new format, these standard contractual clauses have a modular form, addressing 4 different personal data transfer scenarios: (i) from a controller to a processor; (ii) from a controller to a controller; (iii) from a processor to a processor; and (iv) from a processor to a controller. Moreover, relevant is the fact that they directly regulate also onward transfers (offering the possibility for more than two parties to adhere to them and use the clauses throughout the life of the contract) as well as the circumstance that they acknowledge the mandatory assessment on the transfer that the data exporter has to carry out as a consequence of the decision of the Court of Justice of the European Union in the Schrems II case (CJEU judgment in Case C-311/18).

1.3 The validity of the previous versions. The "old" standard contractual clauses (as set out in Decision 2001/497/EC and Decision 2010/87/EU) shall be considered repealed 3 months after the entry into force of the new ones; however, if included in ongoing contracts, they shall remain valid for an additional period of 15 months after the date of repeal.

1.4 What to do. The approval of the new set of standard clauses is an important step towards solving the data transfer puzzle that has emerged in recent years as a result of the ECJ's rulings. The new standard clauses should therefore be adopted as soon as possible, replacing those that may already be in place; the opportunity should then be taken to update, if necessary, the mapping of existing transfers, on which a *data transfer assessment* remains necessary.

Newsletter JUNE 2021

Court of Cassation: compensation for pecuniary damage suffered as a result of unlawful processing of personal data requires a perceptible infringement of the right and proof of the injuries suffered

In its recent judgment no. 16402 of 10th of June 2021, the Court of Cassation reaffirmed two principles of law developed by its own case law regarding the protection of personal data:

(i) the pecuniary damage that can be compensated for the infringement of the legislation on the processing of personal data requires an offence that appreciably affects the scope of the right;

(ii) the compensation for pecuniary damage requires proof, even by presumption, of the prejudice suffered.

1. The minimum prejudice necessary for damages to be compensable

1.1 The threshold of tolerance. First of all, the Court reaffirmed (*see* Court of Cassation nos. 17383 of 20/08/2020 and 11020 of 26/04/2021) the principle according to which non-material damages, even if regarding the violation of a fundamental right protected by articles 2 and 21 of the Constitution and article 8 of the European Convention on Human Rights, cannot be excluded from an assessment on the "severity of the prejudice" and "seriousness of the damage". In line with its own jurisprudence, in fact, the Court of legitimacy has established that also to this right applies the balance with the principle of solidarity provided by Article 2 of the Constitution, of which that of tolerance of the minimum prejudice is an intrinsic derivation. It naturally follows that the mere infringement of the legislation on the protection of personal data cannot give rise to compensation unless it constitutes an unjustifiable prejudice to such right.

1.2 The assessment by the trial judge. As regards the existence and extent of the infringement, the Court points out that such an assessment must take into account the actual nature of the factual matter brought to judicial attention and the specific time-based and social context. In view of this material nature of the assessment, it is a task of the judge of merits to assess whether the offence does not exceed the minimum tolerable threshold or whether the damage is futile, excluding compensation in such cases (*see* Court of Cassation, judgment no. 16133 of 15/07/2014).

2. Proof of damage suffered

2.1 The harmful consequences of the violation must be proved. The Supreme Court then recalls how it has also stated that a damage to the right to privacy, like any other damage to a right, does not exist "*in re ipsa*" but requires that the negative consequences suffered shall be specified and proved (even on a presumptive basis) (*see* Court of Cassation nos. 19434 of 18/07/2019 and 29206 of 12/11/2019). On this point, the Court agrees with the interpretation (carried out by the judge that decided on the merits) according to which it is not sufficient to indicate that one has suffered non-material damage in general, but it is necessary to provide specific allegations on the negative consequences suffered as a result of the processing deemed unlawful, in order to provide useful information to understand the reasons that lead to the non-material damage suffered.

3. Final considerations

3.1 Observations. This judgment, despite referring to article 15 of Legislative Decree 196/2003 (Italian Data Protection Code) in its version prior to the GDPR, establishes a principle applicable

also in relation to article 82 of the GDPR, which has a similar structure, also in terms of burden of proof, to that provided by the combined reading of the provisions in the aforementioned article 15 and in article 2050 of the Italian Civil Code. In fact, according to article 82 paragraph 3 of the GDPR, the controller or the processor shall not be held liable *"if he proves that it is not in any way responsible for the event giving rise to the damage*". However, it remains upon the plaintiff the burden to prove, even by presumptions, the existence of a damage, which is not insignificant. In the present case, neither the judge on the merits nor the Court of Cassation considered that the threshold of seriousness required by law for the granting of a compensation had been fulfilled, according to a constitutionally oriented interpretation that seems to hold up even in the context of the changed legislative scenario. It will therefore remain unlikely, for example, to obtain compensation for having received a few spam emails (on this point, the Supreme Court has already ruled excluding the possibility of compensation for damage resulting from the receipt of 10 spam emails in three years, see Civil Cassation section I, 08/02/2017, n.3311), whereas it will be easier to obtain compensation, for example, by a credit institution that, for lack of adequate security measures, has not prevented third parties from illegally entering the home banking account of one of its account holders.

The one-stop-shop rule in the GDPR does not prevent a local authority from initiating legal proceedings against a subject that has its main establishment not in its territory

In its judgment of 15 June 2021 in Case C-645/19, the Court of Justice of the European Union ("**CJEU**") held that under certain conditions even the national supervisory authority of a Member State other than the one where the controller or processor has its main or single establishment (the lead supervisory authority) may commence or engage otherwise in legal proceedings before a court in its own State, pursuant to Article 58(5) GDPR.

1. The dispute in the main proceedings and the questions referred for a preliminary ruling

1.1 The case. The dispute stemmed from the fact that the Belgian Data Protection Authority brought legal proceedings (acting as legal successor of the President of the Belgian Privacy Commission) against three companies of the Facebook group (Facebook Ireland, Facebook Inc. and Facebook Belgium) for alleged infringements committed in the collection and use of information on the internet browsing behaviour of Belgian internet users, by means of various technologies, such as cookies, social plug-ins or pixels.

1.2 Preliminary ruling on interpretation. The Court of Appeal of Brussels (Hof van beroep te Brussel), called to judge the case, taken into account that Facebook Ireland was the data controller, had doubts about its own jurisdiction to hear the case (in relation to Facebook Ireland and Facebook Inc.), in view of Article 56 GDPR where it provides for the so-called one-stop-shop mechanism. According to such statutory provision, cross-border processing falls under the competence of the lead supervisory authority, i.e. the one competent on the territory of the main or of the single establishment of the controller or processor, which would therefore be the Irish one.

2. The CJEU decision

2.1 The conditions for the competence of a different authority. The CJEU established that the principle enshrined in the GDPR concerning the establishment of a lead authority for cross-border processing do not prevent the supervisory authorities of other Member States from bringing an action against a subject having its main or single establishment on the territory of another Member State, provided that certain conditions are met. In particular, these conditions are the following:

(i) this power is exercised in one of the situations in which the GDPR confers on that supervisory authority the power to adopt a decision finding that such processing is in of the rules contained therein and in that the cooperation and consistency procedures laid down by that regulation are respected.

(ii) the exercise of such powers fall within the territorial scope provided by Article 3 GDPR;

(iii) the object of the legal proceedings is a processing of data carried out in the context of the activities of that establishment and that authority is competent to exercise that power, in accordance with the terms of the answer the first condition. In this regard, in the present case, the CJEU found that the activities of the Facebook group's establishment in Belgium were inextricably linked to the processing of personal data for which the controller is Facebook Ireland and, therefore, the subject of the action necessarily fell within the scope of the activities of that establishment.

3. Final considerations on this ruling

3.1 Observations. This judgment is particularly interesting as it establishes a broad scope of competence for national supervisory authorities and shows how the procedural rules laid down by the Regulation must be interpreted to ensure greater, and not lesser, protection of data subjects' rights. In the light of this, the one-stop-shop mechanism is therefore aimed to ensure coordination and good functioning, but it is not intended to be in itself a limitation of the reasonable competence of each supervisory authority over infringements of the GDPR and of national data protection laws.

Newsletter JUNE 2021

The Data Protection Department of Legance is available to provide any clarifications, also in respect of any specific situation which may be of interest to you.

For further information:

Lucio Scudiero

Managing Associate

T. +39 06.93.18.271
lscudiero@legance.it

Alessandro Amoroso

Associate

T. +39 02.89.63.071
aamoroso@legance.it

or your direct contact at Legance.

Newsletter JUNE 2021

THE FIRM
Legance is an independent Italian law firm with expert, active and result-oriented lawyers, with a strong team spirit that has permitted a flexible and incisive organisational model that, through departments active in all practice areas of business law, offers the right balance between the specialist and the lawyer as a global consultant. Legance comprises over 280 lawyers, working in its Milan, Rome, London and New York offices, and has a diverse and extensive practice covering the following areas: Administrative; Banking & Finance; Compliance; Corporate Finance; Data Protection; Debt Capital Markets; Dispute Resolution; Employment and Industrial Relations; Energy, Project & Infrastructure; Environmental; Equity Capital Markets; EU, Antitrust and Regulation; Financial Intermediaries Regulations; Food; Insurance; Intellectual Property; Investment Funds; Life Sciences & Healthcare; Non Performing Loans; Real Estate; Restructuring and Insolvency; Shipping, Aviation and Transportation; Tax; Telecommunications, Media and Technology; White Collar Crimes. For more information, please visit our website: www.legance.com.