



WORKING PAPER
21/07/2020

Sentenza della Corte di Giustizia dell'Unione Europea C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited e Maximillian Schrems* (“Schrems II”). Implicazioni in materia tributaria?

La Corte di Giustizia dell'Unione Europea (“CGUE”) ha stabilito che i flussi di dati internazionali nell'ambito del regime globale di protezione dei dati dell'Unione Europea, il GDPR, possono continuare a basarsi sulle clausole contrattuali standard dell'UE se adeguatamente monitorate, mentre il *Privacy Shield UE-USA* è stato dichiarato non valido.

Tale pronunciamento può essere valutato nell'ambito del più ampio contesto di tutela dei dati personali, al fine di ipotizzare potenziali ricadute anche in materia fiscale.

Background

Il 16 luglio 2020 la CGUE ha emesso la sentenza nella causa C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited e Maximillian Schrems* (c.d sentenza “Schrems II”), in cui ha confermato la validità delle Clausole Contrattuali Standard per il trasferimento di dati personali a incaricati

European Court of Justice judgement case no. C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited e Maximillian Schrems* (“Schrems II”). Any tax implication?

The Court of Justice of the European Union (“ECJ”) has ruled that international data flows under the European Union’s comprehensive data protection regime, the GDPR, can continue to be based on EU Standard Contractual Clauses if properly monitored, while the EU–U.S. Privacy Shield has been declared invalid.

This judgment can be analyzed in the wider context of personal data protection, in order to verify potential spill-over effects also in tax matters.

Background

On July 16, 2020, the ECJ delivered its judgment in the Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems* (so-called “Schrems II” judgment), confirming the validity of the Standard Contractual Clauses for the transfer of personal

del trattamento al di fuori dell'UE/SEE (“SCCs”), mentre ha dichiarato non compatibile con la normativa comunitaria il *Privacy Shield UE-USA*.

La questione giungeva dinanzi alla CGUE in seguito alla denuncia presentata dal sig. Schrems riguardo al trasferimento di dati personali da parte di *Facebook Ireland Ltd* a *Facebook Inc.* negli Stati Uniti. L'Alta Corte d'Irlanda, rimettendo la questione alla CGUE ha presentato varie questioni pregiudiziali che, in sostanza vertevano:

- sull'interpretazione degli articoli 3(2), 25, 26 e 28(3), della direttiva 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, alla luce dell'articolo 4(2) TUE e degli articoli 7, 8 e 47 della Carta di Nizza;
- sull'interpretazione e validità della decisione 2010/87/UE della Commissione, relativa alle Clausole Contrattuali Standard per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/UE, come modificata dalla decisione di esecuzione (UE) 2016/2297 della Commissione (“**decisione SCC**”);
- sull'interpretazione e validità della decisione di esecuzione (UE) 2016/1250 della Commissione, a norma della direttiva 95/46, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la *privacy* (il c.d. “**Privacy Shield UE-USA**”).

In tale contesto, si deve ricordare che il sig. Schrems era stato già protagonista di un contenzioso pendente innanzi alla CGUE (C-362/14 “*Schrems P*”), la quale ha decretato la violazione dei diritti fondamentali europei, nell'ambito del controllo di massa operato sui dati personali. In detta sede, la CGUE ha dichiarato illegittimo il precedente sistema di protezione dati, denominato “*Safe Harbor*” che facilitava il trasferimento di dati dall'UE agli USA. Nonostante la sostituzione con il sistema noto come *Privacy Shield UE-USA* nel 2016, il ricorrente ha intrapreso la seconda iniziativa legale argomentando come quest'ultimo fosse una versione aggiornata del sistema “*Safe Harbor*” dichiarato illegittimo, giacché nulla di quanto previsto dall'*US Data Surveillance Act* era stato in sostanza modificato.

data to processors outside the EU/EEA (“SCCs”), but declaring as non-compliant, with the EU regulation, the *EU–U.S. Privacy Shield*.

The matter came before the ECJ following a complaint lodged by Mr. Schrems concerning the transfer of personal data by Facebook Ireland Ltd to Facebook Inc. in the United States. The High Court of Ireland decided to refer the issue to the ECJ for a preliminary ruling, which, in essence, concerned:

- the interpretation of Articles 3(2), 25, 26 and 28(3) of 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, read in the light of Article 4(2) TEU and of Articles 7, 8 and 47 of the Nice Charter;
- the interpretation and validity of Commission Decision 2010/87/EU on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (“**the SCC Decision**”); and
- the interpretation and validity of Commission Implementing Decision (EU) 2016/1250 pursuant to Directive 95/46 on the adequacy of the protection provided by the EU-US Privacy Shield (the “**EU–U.S. Privacy Shield**”).

In this context, it is worth recalling that Mr. Schrems had already been the party of a litigation before the ECJ (C-362/14 “*Schrems P*”), which ruled the violation of European fundamental rights, in the context of the mass monitoring of personal data. In particular, the ECJ ruled that the previous data protection system, known as “*Safe Harbor*”, which facilitated the transfer of data from the EU to the USA, was unlawful.

Despite its replacement in 2016 by the system known as *EU-US Privacy Shield*, the applicant filed this further lawsuit arguing that the *EU-US Privacy Shield* in 2016 is a mere updated version of the declared illegitimate “*Safe Harbor*” system, but nothing in the US Data Surveillance Act had been substantially amended.

Le conclusioni dell'AG

Per quanto di nostro interesse, è utile evidenziare come l'AG Saugmandsgaard Øe abbia (a) preliminarmente specificato che il trasferimento dei dati oggetto di giudizio faccia parte dello svolgimento di una attività commerciale, essendo così ad esso applicabile il diritto dell'UE e le normative in materia di privacy e *data transfer*, a prescindere dal successivo utilizzo o trattamento, per qualsivoglia finalità, e (b) concluso per l'assenza di un conflitto tra SCCs e la Carta di Nizza, considerato l'obbligo di sospensione o divieto del flusso dei dati, nei casi di inadeguatezza delle tutele.

Nonostante a seguito di tali conclusioni l'AG non ritenesse necessario valutare la decisione di adeguatezza di quanto stabilito nel *Privacy Shield UE-USA*, questi ha in ogni caso esposto alcune riflessioni circa la decisione 2016/1250, nel caso in cui i giudici avessero deciso di distanziarsi dall'approccio suggerito. Sul punto, riprendendo l'interpretazione già fornita nelle proprie conclusioni del caso *Ministerio Fiscal* (C-207/16), l'AG ha ritenuto determinante (anche per gli altri casi pendenti dinnanzi alla CGUE) il fatto che il diritto dell'UE ed i suoi principi non trovino applicazione alle attività di trattamento per scopi di sicurezza unicamente perseguiti dallo Stato e da autorità pubbliche, senza il coinvolgimento di soggetti privati. Al termine di una complessa disamina della normativa vigente e delle varie casistiche che possono presentarsi di volta in volta, l'AG ha concluso che l'ordinamento statunitense e le tutele introdotte dal regime *Privacy Shield UE-USA*, non forniscono strumenti di accesso alla giustizia e rimedi capaci di garantire il diritto sancito all'art. 47 della Carta di Nizza in maniera sostanzialmente equivalente a quanto stabilito nell'UE.

La sentenza

Con la sentenza in commento, in estrema sintesi, la CGUE ha concluso che:

- il GDPR è applicabile ai trasferimenti di dati tra operatori economici privati, nonostante il fatto che, i suddetti dati possano essere sottoposti a trattamento da parte delle autorità del paese terzo a fini di sicurezza pubblica, di difesa e sicurezza dello Stato;

Opinion of the AG

For the purpose of this paper, it is worth underlying that AG Saugmandsgaard Øe (a) preliminarily specified that the transfer of data subject to judgement has been carried out performing a commercial activity, thus it falls within the scope of EU law and privacy and data transfer regulations, regardless of any subsequent use or processing, for whatever purpose, and (b) concluded that there is no conflict between SCCs and the Nice Charter, given the provided obligation to suspend or prohibit the flow of data, in cases of inadequate safeguards.

Although, based on the above conclusion the AG did not consider as necessary to assess the adequacy of *EU-US Privacy Shield*, he exposed some considerations on the 2016/1250 decision, in case the ECJ would have decided to follow a different approach. On this point, recalling the interpretation already provided in his conclusions in the *Ministerio Fiscal* case (C-207/16), the AG considered as crucial (also for the other cases pending before the ECJ) that EU law and its principles do not apply to data processing activities for security purposes pursued only by the States and public authorities, without the involvement of private parties. At the end of a complex examination of the current legislation and the various cases that may arise from time to time, the AG concluded that the U.S. law, and the protections introduced by the *EU-US Privacy Shield* regime, do not provide adequate remedies capable of ensuring the right granted by Article 47 of the Nice Charter in a manner substantially equivalent to the ones provided in EU.

The decision

With the judgment at hand, in brief, the ECJ concluded that:

- GDPR is applicable to transfers of data between private economic operators, notwithstanding the fact that such data may be processed by the authorities of the third country for public security, defense and state security purposes;

- i mezzi di tutela previsti dal GDPR forniscono garanzie adeguate anche nel caso in cui tali dati siano trasferiti verso un paese terzo sulla base delle SCCs, nella misura in cui tali clausole forniscano un livello di protezione sostanzialmente equivalente a quello Unionale;
 - ai fini di tale valutazione, si devono prendere in considerazione tanto le SCCs convenute tra il titolare o il responsabile del trattamento stabiliti nell'UE e il destinatario del trasferimento stabilito nel paese terzo interessato, quanto, per quel che riguarda un eventuale accesso delle autorità pubbliche di tale paese terzo ai dati personali così trasferiti, gli elementi rilevanti del sistema giuridico di quest'ultimo;
 - a meno che esista una decisione di adeguatezza validamente adottata dalla Commissione europea, qualora un equivalente livello di protezione non possa essere garantito, l'autorità di controllo competente e i titolari del trattamento sono tenuti a sospendere o a vietare un trasferimento di dati, e, se necessario, anche il contratto con l'incaricato del trattamento del paese terzo.
- the means of protection set forth by the GDPR provide adequate safeguards even when such data are transferred to a third country on the basis of SCCs, to the extent that these clauses provide a level of protection substantially equivalent to the Union level;
 - for the purposes of this assessment, it should be taken into consideration both the SCCs agreed between the data controller or controller established in the EU and the recipient of the transfer established in the third country concerned and, regarding potential access by the public authorities of that third country to the personal data thus transferred, of the relevant elements of the latter's legal system;
 - unless there is a valid adequacy decision by the European Commission, if an equivalent level of protection cannot be guaranteed, the competent supervisory authority and the data controller are required to suspend or prohibit a transfer of data and, if necessary, also the contract with the processor in the third country.

On the basis and within the limits of the above, therefore, the ECJ has not found any elements of invalidity of the SCC Decision.

Sulla base e nei limiti di quanto sopra, la CGUE non ha rilevato elementi di invalidità della Decisione SCC.

D'altra parte, la Corte ha ritenuto invalida, con effetto immediato, la decisione di esecuzione (UE) 2016/1250, sull'adeguatezza della protezione offerta dal regime *Privacy Shield UE-USA*. In tal senso, la CGUE ha rilevato come tale regime non preveda limitazioni sufficienti per garantire la protezione dei dati personali dell'UE dall'accesso e dall'uso da parte delle autorità pubbliche statunitensi sulla base della legislazione nazionale statunitense.

On the other hand, the Court invalidated with immediate effect, the Commission Implementing Decision (EU) 2016/1250 on the adequacy of the protection afforded by the *EU-US Privacy Shield* regime. In this respect, the ECJ concluded that this regime does not provide sufficient limitations to ensure the protection of EU personal data from access and use by the US public authorities on the basis of US domestic law.

Considerazioni relative ai possibili impatti in materia fiscale internazionale

È di tutta evidenza che la tematica oggetto della sentenza della CGUE non riguardi direttamente profili di natura fiscale e che il trattamento dei dati personali da parte di società commerciali sia questione ben diversa rispetto allo scambio di dati fiscali dei contribuenti, effettuato da pubbliche autorità, nell'ambito di accordi

Considerations relating to possible international tax impacts

It is clear that the subject matter of the ECJ judgment does not directly concern tax issues and that the processing of personal data by commercial entities is far away from the exchange of taxpayers' tax data by public authorities under international agreements. However, the matter may be relevant if assessed

internazionali. Tuttavia, l'argomento potrebbe assumere una certa rilevanza se valutato nel contesto dei recenti sviluppi di alcune controversie tributarie pendenti dinanzi alla CGEU ed alle corti nazionali.

A tal proposito, nell'ambito dell'ampio tema inerente lo scambio di informazioni fiscali, recentemente l'AG Kokott ha depositato le proprie conclusioni nelle cause riunite C-245/19 e C-246/19, *État du Grand-duché de Luxembourg (Droit de recours contre une demande d'information en matière fiscale)*¹, aventi ad oggetto i limiti alle richieste di informazioni emesse nell'ambito della Direttiva sulla cooperazione amministrativa in materia fiscale (2011/16/EU, "DAC").

In tale sede, è stato argomentato come, in primo luogo, la decisione di un'autorità, nell'ambito di una richiesta di assistenza ai sensi della Direttiva DAC, di richiedere ad un soggetto informazioni relative ad un contribuente o a terzi debba essere impugnabile da parte degli interessati, in quanto l'esclusione della tutela giurisdizionale violerebbe l'art. 47 della Carta di Nizza. Inoltre, l'AG ha precisato come sia onere dell'autorità richiedente motivare in maniera appropriata la propria richiesta di informazioni, affinché l'autorità estera interpellata possa verificare la sussistenza del requisito della "prevedibile pertinenza" all'indagine tributaria in esame, previsto dall'art. 1, comma 1, della Direttiva DAC. In sostanza, è stata affermata la necessità dell'indicazione, nella richiesta di informazioni, di quali siano i fatti giuridicamente rilevanti che si intendono verificare o quantomeno quali siano i sospetti concreti che sono collegati a questi fatti e la loro pertinenza con la verifica fiscale; e che l'obbligo di motivazione risulta tanto più approfondito quanto più sono sensibili le informazioni richieste con riguardo al contribuente. Qualora tali elementi mancassero, una domanda generica o vaga di informazioni da ricercare non rispetterebbe i principi della Direttiva e risulterebbe quindi illegittima alla luce di quest'ultima (c.d. *fishing expedition*). Ma non solo.

Come anticipato, dinanzi a talune corti nazionali pendono contenziosi relativi alla compatibilità dei sistemi di scambio automatico di informazioni, come il CRS (*Common Reporting Standard*) e soprattutto il FATCA (*Foreign Account Tax Compliance Act*), con quanto previsto a livello

in the context of recent developments in some tax disputes pending before the ECJ and national courts.

In this context, in the broad topic of tax information exchange, AG Kokott has recently filed its conclusions in joined cases C-245/19 and C-246/19, *État du Grand-duché de Luxembourg (Droit de recours contre une demande d'information en matière fiscale)*¹, concerning the limits to requests for information issued under the Directive on administrative cooperation in tax matters (2011/16/EU, "DAC").

In this respect, it was argued that, first of all, the decision of an authority, in the context of an application for assistance under the DAC Directive, to request information from a subject concerning a taxpayer or a third party must be challengeable by the persons concerned, since the exclusion of judicial protection would infringe Article 47 of the Nice Charter.

In addition, the AG has explained that the requesting authority must give appropriate grounds for its request for information, so that the foreign requested authority can verify whether the requirement of "foreseeable relevance" to the tax investigation in question, laid down in Article 1(1) of the DAC Directive, is satisfied. Essentially, it has been stated that it is necessary to indicate, in the request for information, what are the legally relevant facts that are under scrutiny or, at least, what are the concrete suspicions that are related to these facts and their relevance for the tax investigation, and that the more sensitive the information required with regard to the taxpayer, the more detailed the obligation to give reasons becomes. Should these elements be missing, a generic or vague request for information to be sought would not respect the principles of the Directive and would therefore be illegitimate in the light of the latter (so-called *fishing expedition*).

Moreover, as anticipated, some disputes are pending before certain national courts concerning the compatibility of the systems of automatic exchange of information, such as the CRS (*Common Reporting Standard*) and the FATCA (*Foreign Account Tax Compliance Act*), with what is foreseen at the Union level in terms of the protection of personal data.

¹ Tax Alert, 7/7/2020 <https://www.fogliandpartners.com/wp-content/uploads/2020/07/7-luglio-2020.pdf>

Unionale in termini di tutela dei dati personali. In specie, sulla base di quanto appreso dalla stampa internazionale, alcuni cittadini hanno contestato la compatibilità con il diritto Unionale di tali sistemi di scambio di informazioni dinanzi a diverse autorità giurisdizionali nazionali. Ad esempio, in un contenzioso tra un cittadino del Regno Unito e l'HMRC sorto a seguito di una denuncia all'autorità di regolamentazione della protezione dei dati Inglese, è stato affermato dal ricorrente come il CRS abbia reso i suoi dati personali vulnerabili ad attacchi *hacker* o a fughe di notizie.

Allo stesso modo, sono state promosse azioni, dinanzi alle corti del Regno Unito, volte a dimostrare come le misure previste dal FATCA siano sproporzionate e ledano i diritti fondamentali alla *privacy* e alla protezione dei dati, in quanto il trasferimento di informazioni ai sensi di tale convenzione non richiede, di per sé, alcun indizio di evasione fiscale e opera indipendentemente da qualsiasi sottostante debito fiscale statunitense.

Da quanto si apprende, i contenziosi si fondano sui principi sanciti dalla normativa dell'Unione Europea e dalla Convenzione europea dei diritti dell'Uomo, secondo cui le limitazioni ai diritti fondamentali alla *privacy* e alla protezione dei dati sono consentite solo nella misura in cui risultino necessarie al raggiungimento di uno specifico obiettivo tutelato dall'ordinamento, come confermato dalla giurisprudenza sia dalla CGUE che dalla Corte suprema del Regno Unito, le quali hanno ritenuto che una verifica sulla sussistenza di tale necessità sia dovuta e rigorosa. A tale proposito, sono state lamentate dalle parti alcune debolezze nel sistema di trasmissione dei dati tra gli enti finanziari, le amministrazioni fiscali e l'IRS (Amministrazione finanziaria USA), in ragione del fatto che i dati possano essere oggetto di *hackeraggio* durante tale trasmissione.

Oltre a tali osservazioni, vengono rintracciati alcuni profili di incompatibilità con diversi principi sanciti dal GDPR (minimizzazione dei dati, liceità del trattamento dei dati, mancanza di garanzie per i trasferimenti di informazioni verso paesi extra-SEE). Infatti, la tematica, oltre a occupare le corti britanniche è stata motivo della presentazione di un contenzioso, innanzi all'autorità per la protezione dei dati personali francese (CNIL), promosso contro l'OCSE ai sensi del GDPR. L'origine di tale procedimento

In particular, on the basis of what has been reported in the international press, some citizens challenged the compatibility with Union law of such systems of exchange of information before various national courts. For instance, in a dispute between a UK citizen and HMRC arising from a complaint to the British Data Protection Authorities, it was stated by the complainant that the CRS made his personal information vulnerable to hacker attacks or leaks.

Similarly, lawsuits have been promoted before United Kingdom courts to demonstrate that the FATCA measures are disproportionate and infringe fundamental rights to privacy and data protection, since the transfer of information under such a convention does not require, on a stand-alone basis, any evidence of tax evasion and operates independently of any underlying US tax liability.

As far as is known, the litigations are based on the principles provided by the European Union law and the European Convention on Human Rights, according to which limitations to fundamental rights to privacy and data protection are allowed only to the extent that they are necessary to achieve a specific objective protected by the law, as confirmed by the case law of both the European Court of Justice and the Supreme Court of the United Kingdom, which have held that such requirements are mandatory and their assessments must be rigorous. In this regard, some weaknesses were complained by the parties in the system of data transmission between financial institutions, tax administrations and the Internal Revenue Service ("IRS", US tax administration), due to the fact that data may be hacked during such transmission.

In addition to these considerations, some incompatibility profiles with several principles established by the GDPR (data minimization, lawfulness of data processing, lack of guarantees for transfers of information to non-EEA countries) have been also pointed out. In fact, the issue, in addition to the British courts, was also the ground for a dispute before the French Data Protection Authority (CNIL) brought against the OECD under the GDPR.

The origin of this proceeding lies in the alleged weakness – for data protection purposes – of the platforms through which the data are

risiede nella argomentata debolezza – ai fini della protezione dei dati personali – delle piattaforme attraverso cui i dati stessi vengono scambiati automaticamente, le quali sono state oggetto di ripetuti attacchi di *hackers*². In aggiunta, occorre notare come la necessità di forti garanzie per i trasferimenti di dati verso gli Stati Uniti sia stata ribadita dall'*European Data Protection Board* nelle linee guida emanate nel gennaio 2020, le quali troverebbero applicazione anche relativamente al FATCA.

Alla luce di tutto quanto sopra, si può osservare come la protezione dei dati personali, oggetto di attenta tutela in ambito europeo, risulti sempre di più questione destinata ad esplicitare la propria efficacia in maniera “trasversale”, dovendosi domandare se ciò possa, in qualche misura, assumere rilevanza, anche in ambito fiscale, pur nel contesto di un doveroso bilanciamento di valori e di interessi meritevoli di tutela; sarà opportuno, nel futuro, un attento monitoraggio dell’evoluzione di tale giurisprudenza, sia ai fini delle possibili implicazioni in tema di tutela dei contribuenti, sia per stabilire la coerenza dei sistemi di scambio automatico di informazioni, con la protezione dei dati personali sensibili.

exchanged automatically, which have been subject to repeated hacker² attacks.

In addition, it should also be noted that the need for a strong safeguard for data transfers to the United States has been reiterated by the *European Data Protection Board* in the guidelines issued in January 2020, which would also apply to FATCA.

In the light of all the above, it is worth observing that the protection of personal data, which is the subject of careful attention in the European context, is becoming an issue destined to impact the regulations in a compressive and transversal manner, and it would be useful to wonder whether this could have some ramifications also in the tax area, even in the context of a necessary balance of values and public interests worthy of protection; it will be worth, in the future, closely monitoring the development of this case law, in terms of potential implications for the protection of taxpayers and in order to assess the consistency of systems for the automatic exchange of information with the protection of sensitive personal data.

* * *

Foglia & Partners è a Vostra disposizione per ogni ulteriore chiarimento ed approfondimento in merito ai temi affrontati.

Foglia & Partners is at your disposal for any further clarification and in-depth study of the issues addressed.

Contatti:

Contacts:

Email: home@fptax.it Web: fogliandpartners.com
Roma, Via dei Prefetti 17, Tel: +39 06 68300655
Milano, Largo Ildefonso Schuster 1, Tel: +39 02 09994690

Il presente documento ha finalità meramente informativa e non può essere inteso, in alcun modo, quale parere legale.

This document is for information purposes only and cannot be construed in any way as legal advice.

² <https://www.oecd.org/tax/transparency/statement-on-the-data-breach-in-the-national-revenue-agency-of-bulgaria.htm>; <https://www.bbc.com/news/technology-49015511>