Consultazione pubblica nell'ambito delle Linee guida 07/2022 sulla certificazione come strumento per i trasferimenti (consultazione pubblica di riferimento 07/2022)". Contributo alla bozza di Linee guida 07/2022 sulla certificazione come strumento per i trasferimenti

Public consultation in the framework of the Guidelines 07/2022 on certification as a tool for transfers (public consultation reference 07/2022). Contribution to draft Guideline 07/2022 on certification as a tool for transfers.

Dr. Francisco Garcia-Garrido.
Lawyer, PhD Administrative Law & Legal Compliace (ReNorm S.r.l.) – Expert EDPB

Strumenti giuridici vincolanti ed esecutivi tra attori pubblici e privati. Clausole contrattuali tipo che tentano di coprire il vuoto normativo in materia. Accordi internazionali di limitata e dubbiosa applicazione nella realtà nazionale. Codici di condotta, altri strumenti quasi regolatori e contratti privati fra attori (c.d. nomine ex art. 28 GDPR 2016/679).

Binding and enforcement legal mechanisms between public and private actors. Standard contractual clauses attempting to cover the legal framework vacuum. International agreements of limited and doubtful application in national reality. Codes of conduct, other meta-regulatory instruments and private contracts between actors (so-called appointments under Article 28 GDPR 2016/679).

Tutti questi meccanismi cercano di risolvere, in maniera alquanto dubbiosa, la problematica relativa al trasferimento dei dati personali oltre lo Spazio Economico Europeo (SEE) oppure verso un'organizzazione internazionale. In particolare, il considerando 6 del Regolamento (UE) 2016/679 mette in luce come "la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali".

All these instruments attempt to resolve, somewhat dubiously, the issue of the transfer of personal data beyond the European Economic Area (EEA) or to an international organization. In particular, recital 6 of Regulation (EU) 2016/679 highlights how "the speed of technological change and globalization bring new challenges for the protection of personal data".

Tuttavia, il regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché i susseguenti atti giuridici vincolanti e non – di origine europea nonché emanati dalle autorità amministrative indipendenti di ogni singolo Stato membro – tentano di far fronte ad una problematica che va oltre i confini nazionali ed europei.

However, the Regulation on the protection of individuals with regard to the processing of personal data as well as the subsequent binding and non-binding legal acts - of European origin as well as issued by the independent administrative authorities of each individual Member State - attempt to address an issue that goes beyond national and European borders.

The European Data Protection Board (EDPB) is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union and promotes cooperation between the EU's data protection authorities.

The EDPB is established by the General Data Protection Regulation (GDPR) and is based in Brussels. The EDPB is composed of representatives of the EU national data protection authorities (national Supervisory Authorities), and the European Data Protection Supervisor (EDPS).

The supervisory authorities of the EFTA EEA States (IS, LI, NO) are also members with regard to GDPR-related matters and without the rights to vote and to be elected as chair or deputy chairs. The European Commission and - with regard to GDPR-related matters - the EFTA Surveillance Authority have the right to participate in the activities and meetings of the Board without voting rights.

The EDPB has a Secretariat, which is provided by the EDPS. A Memorandum of Understanding determines the terms of cooperation between the EDPB and the EDPS.

Link: https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en

Lo stesso considerando 6 del GDPR riconosce come "[l]a tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali" / The same recital 6 of the GDPR recognizes how "[t]he technology has transformed the economy and social relations and should further facilitate the free flow of personal data within the Union and their transfer to third countries and international organizations, while ensuring a high level of protection of personal data".

E rieccoci di nuovo, di fronte al problema.

And here we are again. Once again faced with the problem.

La normativa europea – sebbene preveda la possibilità di trasferire dati personali verso paesi terzi – impone ad esportatori ed importatori che operano nel commercio dei dati personali un ventaglio di condizioni non definite con chiarezza. Tali misure hanno, quale denominatore comune, la necessità di garantire, ove possibile, un adeguato livello di protezione dei dati oltre l'UE, essenzialmente equivalente a quello assicurato all'interno dello SEE.

In assenza di misure determinate e vincolanti, di diretta applicazione a livello nazionale, il Comitato Europeo per la Protezione dei Dati Personali (EDPB), consapevole dell'assenza di strumenti giuridici in grado di regolamentare e tutelare il trasferimento dei dati oltre l'UE, aveva emanato le c.d. "Linee guida EDPB 4/2021 sui codici di condotta come strumenti per i trasferimenti verso paesi terzi od organizzazioni internazionali" recepite dalla maggior parte degli Stati a cui si applicano le disposizioni del GDPR.

L'EDPB, in occasione della 41° sessione plenaria, aveva inoltre adottato le c.d. "raccomandazioni sulle misure supplementari per i trasferimenti di dati a seguito della famosa Sentenza Schrems II".

La Sentenza Schrems II ha trasformato radicalmente il panorama giuridico recante i trasferimenti di dati personali oltre l'UE, ovvero verso gli Stati Uniti. Secondo la Corte di giustizia dell'Unione europea (CGUE), nella "causa C-311/18 – Data Protection Commissioner contro Facebook Ireland Ltd e Maximillian Schrems", i requisiti della normativa interna degli Stati Uniti – e in particolare taluni programmi che consentono l'accesso da parte delle autorità pubbliche statunitensi, per finalità di sicurezza nazionale, ai dati trasferiti dall'UE verso gli Stati Uniti – comportano limitazioni della protezione dei dati personali che non sono configurate in modo da soddisfare requisiti equivalenti a quelli richiesti nel diritto dell'UE.

Negli ordinamenti giuridici austriaco, francese e italiano, le rispettive autorità amministrative indipendenti – dotate di discrezionalità eminentemente tecnica – hanno imposto delle limitazioni al trasferimento di dati personali oltre l'UE.

Nel recentissimo caso italiano, l'Autorità Garante per la Protezione dei Dati Personali – con provv. del 9 giugno 2022 – ha ammonito la società Caffeina Media Srl per aver trasferito dati personali a Google LLC (con sede legale negli Stati Uniti). A seguito di una efficace attività istruttoria, il Garante italiano – che si è sommato alla medesima decisione presa anche dalla Datenschutzbehörde austriaca e dalla Commission nationale de l'informatique et des libertés francese – ha ritenuto illegittimo il trattamento effettuato da Google LLC ribadendo che il sito web che utilizza il servizio Google Analytics (GA), senza le garanzie previste dal Regolamento (UE) 2016/679, viola la normativa sulla protezione dei dati perché trasferisce i dati degli utenti negli Stati Uniti, Paese privo di un adeguato livello di protezione.

Il progressivo abbandono dei confini nazionali e l'internazionalizzazione delle aziende, l'utilizzo generalizzato di strumenti informatici a supporto delle (S)ocietà e l'opportunità nonché necessità delle strutture pubbliche e private di contrattualizzare con soggetti privati transnazionali alcuni servizi (es. rete globale di server, analisi e produzione di statistiche nonché strumenti analitici, cloud intelligenti con sede oltre l'UE) sono solo alcuni esempi che ci portano a comprendere l'emergenza di dover trovare uno strumento in grado di tutelare la sicurezza dei dati personali oggetto di trattamento al di là dei confini dello SEE. Le limitazioni possono restringere una determinata attività che, però,

European law - although providing for the possibility of the transfer of personal data to third countries - imposes a set of conditions on exporters and importers involved in the trade of personal data that are not clearly defined. These have, as a common denominator, the need to ensure, where possible, an adequate level of data protection beyond the EU, essentially equivalent to that provided within the EEA.

In the absence of determined and binding measures of directly applicable at the domestic law, the European Data Protection Board (EDPB), aware of the absence of legal instruments capable of regulating and protecting the transfer of data beyond the EU, had issued the so-called 'EDPB Guidelines 4/2021 on codes of conduct as instruments for transfers to third countries or international organisations', which have been transposed by most of the states to which the provisions of the GDPR apply.

The EDPB, at its 41st plenary session, had also adopted the so-called "recommendations on additional measures for data transfers following the notorious Schrems II Judgment".

The Schrems II Judgment has radically transformed the legal framework surrounding personal data transfers beyond the EU, i.e. to the United States. According to the Court of Justice of the European Union (CJEU), in 'Case C-311/18 - Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems', the requirements of US domestic law - and in particular certain programmes allowing access by US public authorities, for national security purposes, to data transferred from the EU to the US - entail limitations on the protection of personal data that are not designed to meet equivalent requirements to those required under EU law.

In the Austrian, French and Italian legal systems, the respective independent administrative authorities - endowed with eminently technical discretion - have imposed restrictions on the transfer of personal data beyond the EU.

In the very recent Italian case, the Italian Data Protection Authority - with a provision of 9 June 2022 - admonished the company Caffeina Media Srl for having transferred personal data to Google LLC (with registered office in the United States). Following an effective preliminary activity, the Italian Garante - which added to the same decision taken also by the Austrian Datenschutzbehörde and the French Commission nationale de l'informatique et des libertés - deemed unlawful the processing carried out by Google LLC, reiterating that the website using the Google Analytics (GA) service, without the guarantees provided for by Regulation (EU) 2016/679, violates data protection legislation because it transfers users' data to the United States, a country lacking an adequate level of protection.

The progressive abandonment of national borders and the internationalisation of companies, the generalised use of IT tools to support (S)ocieties, and the opportunity and need for public and private structures to contract certain services (e.g. global network of servers, analysis and production of statistics as well as analytical tools, intelligent clouds based beyond the EU) with transnational private entities are just a few examples that lead us to understand the urgency of having to find an instrument capable of protecting the security of personal data being processed beyond the borders of the EEA. Restrictions may restrict a certain activity that, however, follows the path of

segue il percorso di un processo di mondializzazione economica, commerciale, sociale e culturale in continua evoluzione.

Si pensi al paradosso di versare un bicchiere di acqua su una superficie molto porosa e pretenderne il non assorbimento.

Non ci sono garanzie vere e proprie ma soltanto limitazioni.

L'articolo 44 del GDPR recante il principio generale per il trasferimento, sulla base dei considerandi 101 e 102, rappresenta la prima limitazione volta a incidere sulle posizioni giuridiche dei titolari e responsabili del trattamento di dati personali con sede legale all'interno dello SEE che intendono trasferire dati personali oltre tali confini. Ecco una delle prime limitazioni e, allo stesso tempo, contraddizioni alla luce del considerando 6 sopra citato.

Per il buon funzionamento del mercato interno ed esterno dovrebbe essere garantita la libera circolazione dei dati personali e non limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali. Questo dovrebbe essere il principio.

Il GDPR stabilisce che i trasferimenti di dati personali verso Paesi non appartenenti allo SEE o verso un'organizzazione internazionale sono consentiti a condizione che l'adeguatezza del Paese terzo o dell'organizzazione sia riconosciuta tramite decisione della Commissione europea (art. 45 del Regolamento UE 2016/679). Ciononostante, a livello europeo il trasferimento di tali dati è preceduto da misure prettamente formali che trovano a malapena spazio nel quadro normativo di ogni singolo Stato membro.

Sebbene la recentissima decisione di esecuzione (UE) 2021/914 della Commissione del 4 giugno 2021 ha fornito le clausole contrattuali tipo per permettere il trasferimento di dati personali verso paesi terzi a norma del GDPR, tali clausole non costituiscono una garanzia adeguata bensì uno strumento di responsabilizzazione o di *accountability* in capo ai titolari del trattamento. Si tratta di una mera formalità.

E ora arriva il soft law: strumenti di certificazione e di regolamentazione procedimentalizzata ai sensi del GDPR.

Fino ad oggi, l'onere di responsabilizzazione e di accountability è in capo ai titolari del trattamento. Nel caso in specie, in capo alle strutture pubbliche o private che intendono trasferire dati personali oltre lo SEE: dalla nomina ex art. 28 GDPR alle clausole tipo allegate al contratto di servizio. Come sopra accennato, nella maggior parte dei casi sono "tutte formalità" prive di vere e proprie garanzie.

L'art. 46 comma 2 b) del GDPR apre la porta ai c.d. strumenti di certificazione privata, approvati a norma dell'art. 42, unitamente all'impegno vincolante ed esigibile del titolare o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati. Invero si tratta di uno strumento che pone al centro dell'attenzione la struttura pubblica o privata che effettua il trasferimento dei dati oggetto di trattamento oltre lo SEE, indipendentemente dal ruolo che assume nell'organigramma privacy.

Come sappiamo, i soggetti che operano per conto del Titolare, ovvero i responsabili del trattamento localizzati oltre lo SEE, possono anche avvalersi di strutture esterne, terze, che assumono a loro volta il ruolo di sub-responsabili ai sensi dell'art. 28 del GDPR.

an ever-changing process of economic, commercial, social and cultural globalisation.

Think of the contradiction of pouring a glass of water on a very porous surface and expecting it not to be absorbed.

There are no real guarantees, only limitations.

Article 44 of the GDPR on the general principle for transfers, based on recitals 101 and 102, is the first limitation aimed at affecting the legal positions of data controllers and processors of personal data with a registered office within the EEA who intend to transfer personal data beyond those borders. This is one of the first limitations and, at the same time, contradictions in the light of recital 6 cited above.

For the good functioning of the internal and external market, the free movement of personal data should be guaranteed and not restricted or prohibited on grounds of the protection of natural persons with regard to the processing of personal data. This should be the principle.

The GDPR states that transfers of personal data to non-EEA countries or to an international organisation are permitted provided that the adequacy of the third country or organisation is recognised by a decision of the European Commission (Art. 45 of EU Regulation 2016/679). Nevertheless, at the European level the transfer of such data is preceded by purely formal measures that barely find a place in the regulatory framework of each individual Member State.

Although the very recent Commission Implementing the Decision (EU) 2021/914 of 4 June 2021 provided the standard contractual clauses to allow the transfer of personal data to third countries under the GDPR, these clauses do not constitute an adequate guarantee but rather an instrument of responsibility or accountability on the part of data controllers. They are a simple formality.

And now comes soft law: certification tools and procedural regulation under the GDPR.

The duty of responsibility and accountability lies with data controllers. In this case, it is in the hands of public or private facilities that intend to transfer personal data beyond the EEA: from the appointment under Article 28 GDPR to the standard clauses attached to the service contract. As mentioned above, in most cases these are 'all formalities' without any real guarantees.

Article 46(2)(b) of the GDPR opens the door to so-called private certification schemes, approved under Article 42, together with a binding and enforceable commitment by the controller or processor in the third country to apply appropriate safeguards, including with regard to the rights of data subjects. Indeed, this is an instrument that puts the focus on the public or private entity that transfers the data being processed beyond the EEA, irrespective of the role it plays in the privacy organisation chart.

As we know, the entities acting on behalf of the data controller, i.e. the data processors located beyond the EEA, may also make use of external, third-party structures, which in turn take on the role of sub-processors within the meaning of Article 28 of the GDPR.

La possibilità di vincolare gli esportatori ad adottare garanzie adeguate al trasferimento di dati personali verso paesi terzi od organizzazioni internazionali in virtù di una certificazione è stata studiata dall'EDPB.

Le recentissime linee guida 07/2022 sulla certificazione come strumento per i trasferimenti (in consultazione pubblica fino al 30 settembre 2022) forniscono indicazioni sull'applicazione della c.d. certificazione per i trasferimenti dei dati oltre l'UE.

Le linee guida proposte dagli expert dell'EDPB, in primo luogo, chiariscono che per ottenere la certificazione, gli esportatori devono essere in grado di garantire la conformità alle disposizioni generali del GDPR ed in particolare le disposizioni del Capo V del Regolamento stesso. Tuttavia, come sopra premesso, tale controllo grava sul Titolare del trattamento ovvero sulla struttura europea che ricorre ad un esportatore che effettua il trattamento oltre lo SEE.

Di particolare importanza sono le sezioni II, III e IV delle sopracitate linee guida in fase di consultazione.

La sezione II contiene una guida all'attuazione dei requisiti di accreditamento da parte degli esportatori. Tale sezione mette in luce il ruolo dell'EDPB quale ente dotato di potere per approvare i criteri di certificazione a livello SEE e di fornire pareri sui progetti di decisione delle autorità nazionali. Di particolare interesse è il ruolo dell'Ente Unico di Accreditamento ovvero l'organismo nazionale autorizzato dallo Stato a svolgere attività di accreditamento. In Italia è Accredia, in Spagna Aenor, in Francia il Comitato Cofrac. Tali organismi – prima dell'attestazione – verificano i servizi ed i sistemi di gestione delle strutture con sede legale oltre lo SEE per effettuare il trasferimento e ne attestano la conformità alle norme, volontarie e obbligatorie, mediante le attività di certificazione, di ispezione e di prova. L'EDPB identifica altresì la norma ISO 17065 che stabilisce i requisiti che un organismo di certificazione deve soddisfare per dimostrare di operare in modo competente, coerente ed imparziale.

La sezione III presenta i criteri specifici di certificazione, determinati sulla base della norma ISO 17065 e dell'interpretazione delle Linee Guida 4/2018 dell'EDPB. Il comma 34 della sezione III identifica una questione di importante valore relativa ai requisiti di processo: nello specifico, il processo di certificazione dev'essere effettuato in relazione al trattamento che avverrà nei paesi terzi in cui si pretende effettuare il trasferimento e – oltre a dover tenere conto della normativa applicabile e delle politiche nazionali – effettuare in loco eventuali audit ispettivi all'esportatore.

Dunque, la certificazione è condizionata dall'attività di monitoraggio ed ispettiva effettuata sia dal titolare del trattamento che dall'organismo di accreditamento, tenuto a valutare l'adeguatezza dell'esportatore alla normativa UE.

La guida fornita dall'EDPB relativamente all'attuazione dei criteri di certificazione contiene altresì specifiche indicazioni sul principio di trasparenza ed i diritti degli interessati perché possa essere rilasciata la certificazione. Nello specifico, il comma 41 della sezione III "suggerisce" che i criteri di certificazione devono richiedere che vengano date informazioni sulle attività di trattamento, che vengano garantiti agli interessati i diritti di cui agli artt. 15-22 del GDPR e che prevedano un'adeguata procedura di gestione dei reclami da parte della struttura in possesso di una certificazione. Ovviamente, tutti questi requisiti devono essere stabiliti e correttamente definiti all'interno di un accordo contrattuale tra titolare e responsabile del trattamento, ovvero tra importatore ed esportatore dei dati.

The possibility of binding exporters to adopt appropriate safeguards when transferring personal data to third countries or international organisations by virtue of a certification has been explored by the EDPB.

The recent guidelines 07/2022 on certification as a tool for transfers (in public consultation until 30 September 2022) provide guidance on the application of so-called certification for data transfers beyond the EU.

The guidelines proposed by the EDPB experts firstly clarify that in order to obtain certification, exporters must be able to ensure compliance with the general provisions of the GDPR and in particular the provisions of Chapter V of the Regulation itself. However, as stated above, this check is the responsibility of the data controller or the European structure that uses an exporter that carries out processing beyond the EEA.

Particularly important are Sections II, III and IV of the above-mentioned guidelines in consultation.

Section II contains guidance on the implementation of accreditation requirements by exporters. This section highlights the role of the EDPB as the body with the power to approve certification criteria at EEA level and to give opinions on draft decisions of national authorities. Of particular interest is the role of the Ente Unico di Accreditamento, i.e. the national body authorised by the state to carry out accreditation activities. In Italy this is Accredia, in Spain Aenor, in France the Cofrac Committee. These bodies - prior to the attestation - verify the services and management systems of facilities with registered offices outside the EEA to carry out the transfer and certify their compliance with standards, both voluntary and mandatory, through certification, inspection and testing activities. The EDPB also identifies ISO 17065, which sets out the requirements that a certification body must fulfil to demonstrate that it operates in a competent, consistent and impartial manner.

Section III presents the specific certification criteria, determined on the basis of ISO 17065 and the interpretation of EDPB Guideline 4/2018. Paragraph 34 of Section III identifies an important issue regarding process requirements: specifically, the certification process must be carried out in relation to the processing that will take place in the third country to which the transfer is to be made and - in addition to having to take into account the applicable legislation and national policies - carry out on-site audits of the exporter.

Certification is conditional on monitoring and inspection activities carried out by both the data controller and the accreditation body, which is required to assess the exporter's compliance with EU regulations.

The guidance provided by the EDPB on the implementation of certification criteria also contains specific indications on the principle of transparency and the rights of data subjects for certification to be granted. Specifically, paragraph 41 of Section III 'suggests' that the certification criteria must require that information be given about processing activities, that data subjects be guaranteed the rights set out in Articles 15-22 of the GDPR, and that they provide for an adequate complaint handling procedure on the part of the facility holding a certification. All these requirements must be established and properly defined within a contractual agreement between data controller and data importer and data exporter.

La sezione IV riguarda gli impegni vincolanti ed eseguibili da attuare. La possibilità di ricorrere alla certificazione privata costituisce un impegno assunto tramite un contratto. Secondo l'EDPB, questa appare come la soluzione più semplice in quanto potrebbero essere utilizzati anche altri strumenti a condizione che titolare e responsabile del trattamento siano in grado di dimostrare il carattere vincolante ed esecutivo di tali mezzi.

Le linee guida dell'EDPB sulla certificazione come strumento per i trasferimenti sono senz'altro uno strumento molto utile nell'ambito della problematica appena illustrata.

Tuttavia, la certificazione non è la soluzione a tutti i problemi. La certificazione come strumento per i trasferimenti di dati personali oltre l'UE è un meccanismo alternativo, di natura volontaria, a cui ambiscono prevalentemente le strutture meglio organizzate, che contano con maggiore potere e risorse nel contesto globale. Nell'ambito dei principali big tech sono Amazon, Microsoft Corporation e Apple Inc. le società tecnologiche con sede legale negli Stati Uniti maggiormente interessate ad avviare il percorso di certificazione per i trasferimenti oltre lo SEE.

Relativamente all'iter procedurale, va tenuto in considerazione un aspetto di non minore rilevanza.

Sebbene le stesse linee guida proposte dall'EDPB specifichino che "la certificazione è volontaria e disponibile attraverso un processo trasparente", va però avvertito l'EDPB in quanto vi è un refuso al comma 24 delle Linee Guida. L[l]a procedura per l'ottenimento della certificazione non è volontaria bensì *condicio sine qua non* per ottenerla. L'EDPB deve tenere in considerazione che la procedura di certificazione è l'iter obbligatorio e la sequenza ordinata di steps finalizzata all'ottenimento da parte dell'esportatore della certificazione. In poche parole: la certificazione è volontaria ma la procedura per ottenerla è da ritenersi obbligatoria.

Un importantissimo tassello nell'ambiguo mondo delle certificazioni è il collegamento con la realtà giuridica di ogni singolo Stato membro ed i poteri di cui gode ogni autorità nazionale. La certificazione per il trasferimento dei dati oltre l'UE richiede necessariamente un dialogo concreto con il diritto positivo, al fine di non confinarla a meccanismo isolato che si pone in contrapposizione a ciò che è stato normativamente imposto dall'ordinamento giuridico nazionale. Dall'altro lato, vi sono i compiti delle autorità garanti volti ad evitare una controversia nell'ambito del trasferimento di dati personali extra UE. Oltre a controllare che i trattamenti di dati personali siano conformi al Regolamento nonché a leggi e regolamenti nazionali, le autorità nazionali saranno tenute a ponderare i propri poteri e a confrontarsi con altri soggetti privati ed organismi nazionali nonché europei legittimati, pertanto, a valutare gli effettivi criteri di certificazione.

Contributo di Francisco Garcia-Garrido nell'ambito della procedura "Consultazione pubblica - Linee guida 07/2022 sulla certificazione come strumento per i trasferimenti.

Section IV deals with binding and enforceable obligations to be implemented. The possibility of using private certification constitutes a commitment made by means of a contract. According to the EDPB, this appears to be the simplest solution since other means could also be used provided that the controller and processor are able to demonstrate the binding and enforceable nature of these means.

The EDPB guidelines on certification as a tool for transfers are undoubtedly a very useful tool in the context of the issue just outlined.

However, certification is not the solution to all problems. Certification as a tool for personal data transfers beyond the EU is an alternative mechanism of a voluntary nature, which is mostly sought after by the best organised structures with the most power and resources in the global context. Within the major big tech companies, Amazon, Microsoft Corporation and Apple Inc. are the most interested in starting the certification route for transfers beyond the EEA.

Concerning the procedure, one very important aspect must be taken in consideration.

Although the EDPB Guidelines themselves specify that "certification is voluntary and available through a transparent process", the EDPB should be warned that there is a typo in paragraph 24 of the Guidelines. The procedure for obtaining certification is not voluntary, but a condition sine qua non for obtaining it. The EDPB must consider that the certification procedure is the mandatory process and orderly sequence of steps for the exporter to obtain certification. In a nutshell: certification is voluntary but the procedure to obtain it is mandatory.

A very important element in the ambiguous world of certification is the connection with the legal framework of each individual Member State and the powers enjoyed by each national authority. Certification for the transfer of data beyond the EU necessarily requires a concrete dialogue with positive law, in order not to confine it to an isolated mechanism that stands in opposition to what has been normatively imposed by the national legal system. On the other hand, there are the tasks of the supervisory authorities aimed at avoiding litigation in the context of the transfer of personal data outside the EU. In addition to checking that personal data processing complies with the regulation as well as with national laws and regulations, the national authorities will be required to weigh their powers and to compare them with other private entities and national as well as European bodies that are entitled, therefore, to assess the actual certification criteria.

Contribution by Francisco Garcia-Garrido in the framework of the procedure "Public Consultation - Guidelines 07/2022 on certification as a tool for transfers.

Contribution of Francisco Garcia-Garrido in the framework of the procedure "Public Consultation - Guidelines 07/2022 on Certification as a Tool for Transfers Francisco Garcia-Garrido is a Spanish lawyer, PhD in Administrative Law at the University of Trento and Legal Consultant at ReNorm S.r.l. He has been working with the EDPB since 2022 as European Expert in the field of personal data protection.