

## **Transfer of personal data to third countries or international organisations: the solution of italian government**

*Gaetana Natale\**

In this panel the topic is subject rights. It is important a practical approach to understand and analyse the solutions of the problems in the different cases, following best practices.

The subject rights are crucial in the transfers of data both on the basis of an adequacy decision where the Commission has decided that the third country or the international organization in question ensures an adequate level of protection and transfers subject to appropriate safeguards or binding corporate rule or code of conduct and certification, general data protection clauses such a transfer shall not require any specific authorisation. The first level of protection is awareness of subject right. It is important to individuate the centre of imputation of liability, strict liability in processing data.

When assessing the adequacy of the level of protection, after Shield case and safe harbor, the Commission shall, in particular, take account of: rule of law, respect of human rights and fundamental freedom, relevant legislation both general and sectorial, data protection rules, security measures, case law as well as effective and enforceable data subjects rights and effective and administrative, judicial redress for the data subjects whose personal data are being transferred. International organisations are a trustworthy system for personal data processing.

Important tool is enforcement: private and public enforcement by independent supervisory, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member states in Europe and international organisations observing one stop shop with some mitigation. This protection is dynamic and not static with following review. The privacy is not formal compliance, but substantial protection, defence, safeguard of fundamental rights. Lastly it is clear that the system envisaged is based on the subsidiarity and proportionality. The principles of subsidiarity and proportionality should be fully respected as should fundamental rights.

I will explain you some examples of accountability, proportionality, privacy by design and default. It is important the rule of Data Protection Office

---

(\*) Avvocato dello Stato, Professore a contratto di Sistemi Giuridici Comparati, Consigliere giuridico del Garante per la Privacy.

*Costituisce il presente scritto la relazione presentata il 12 maggio u.s. dall'Autrice ad un convegno organizzato dall'Agenzia ONU World Food Programme (WFP) e da European Data Protection Board (EDPB) in tema di protezione dei dati e organizzazioni internazionali.*

both his surveillance, supervision activity and advising activity for subjects right.

1. UNICEF - As reported on page 79 in the 2019 Annual Report: *“The Ministry of the Interior consulted the Privacy Guarantor about a project initiated with Unicef in relation to the strengthening of the reception and protection system for unaccompanied foreign minors (MSNA) which provides for the promotion of foster care paths, as an alternative measure for reception and social inclusion, and the coordination of the institutions responsible for taking care of unaccompanied foreign minors. The agreement scheme prepared by the Ministry for project management contains specific references to compliance with the GDPR and the Privacy Code. Considering that Unicef cannot be the recipient of obligations deriving from regulations issued by sovereign states or the European Union - such as the GDPR and the Code - in consideration of the immunities and privileges recognized to international organizations, the Ministry of the Interior asked the Guarantor if the legislation on the protection of personal data applies to it. The Office highlighted that the Ministry must verify that the processing is carried out in compliance with the applicable principles (articles 5, 6, 9 and 10 of the GDPR and 2-ter, 2-sexies, 2-septies, 2-octies of the Code) and identify on the basis of which assumptions, provided for by art. 44-50 of the RGPD, the flow of personal data to the international organization is carried out. In this context, it was recalled that based on the orientation expressed by the Cepd (guidelines 2/2018 on the exceptions referred to Article 49 of the GDPR, adopted on 25 May 2018), data controllers who intend to transfer personal data towards third countries or international organizations, should first explore the possibility of using one of the guarantee mechanisms for the transfer as provided by Articles 45 and 46 of the GDPR (adequacy decisions or adequate guarantees) and, only if this is not possible, make use of the the derogation hypotheses indicated in art. 49, par. 1, of the GDPR (1). These exceptions, in fact, “should be interpreted stric-*

---

(1) **Art. 44 GDPR:** “1. Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.

2. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined”.

**Art. 45 GDPR:** “1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements: the rule of law, respect for human rights and fundamental freedoms,

*tly, so that the exception does not turn into the rule” (art. 49; see guidelines 2/2018 cit.; see also WP114 Working document on a common interpretation of art. 26, par. 1 of directive 95/46/EC”, adopted by the Art. 29 Group on 25 November 2005). In the specific case, in order to verify whether the hypothesis of derogation provided by art. 49, par. 1, lett. d), of the GDPR (“the transfer is necessary for important reasons of public interest”), the public interest pur-*

---

relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred; the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

3. The Commission, after assessing the adequacy of the level of protection, may decide, by means of implementing act, that a third country, a territory or one or more specified sectors within a third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2 of this Article. The implementing act shall provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority or authorities referred to in point (b) of paragraph 2 of this Article. The implementing act shall be adopted in accordance with the examination procedure referred to in Article 93.

4. The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the functioning of decisions adopted pursuant to paragraph 3 of this Article and decisions adopted on the basis of Article 25 of Directive 95/46/EC.

5. The Commission shall, where available information reveals, in particular following the review referred to in paragraph 3 of this Article, that a third country, a territory or one or more specified sectors within a third country, or an international organisation no longer ensures an adequate level of protection within the meaning of paragraph 2 of this Article, to the extent necessary, repeal, amend or suspend the decision referred to in paragraph 3 of this Article by means of implementing acts without retro-active effect. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93. On duly justified imperative grounds of urgency, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 93.

6. The Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to paragraph 5.

7. A decision pursuant to paragraph 5 of this Article is without prejudice to transfers of personal data to the third country, a territory or one or more specified sectors within that third country, or the international organisation in question pursuant to Articles 46 to 49.

8. The Commission shall publish in the Official Journal of the European Union and on its website a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

9. Decisions adopted by the Commission on the basis of Article 25 of Directive 95/46/EC shall remain in force until amended, replaced or repealed by a Commission Decision adopted in accordance with paragraph 3 or 5 of this Article”.

*sued must be recognized by Union law or by the law of the Member State (Article 49, paragraph 4). In this context, it was recalled that the existence of an international agreement or convention that establishes a specific objective, to be favored with international cooperation, “must be considered as an indica-*

---

**Art. 46 GDPR:** “1. In the absence of a decision pursuant to Article 45, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by: a legally binding and enforceable instrument between public authorities or bodies; binding corporate rules in accordance with Article 47; standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93; standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93; an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects’ rights; or an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects’ rights.

3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by: contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. 2Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article”.

**Art. 47 GDPR:** “1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they: are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees; expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least: the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members; the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question; their legally binding nature, both internally and externally; the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules; the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules; the acceptance by the controller or processor esta-

*tor for the purpose of assessing the existence of a public interest pursuant to art. 49, par. 1, lett. d), provided that the European Union or the Member States have signed this agreement or convention". It was also suggested to the Ministry to evaluate the existence of internal policies at Unicef or the adherence*

---

blished on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage; how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14; the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling; the complaint procedures; the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority; the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority; the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j); the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and the appropriate data protection training to personnel having permanent or regular access to personal data.

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. 2 Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2)".

**Art. 48 GDPR:** "Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter".

**Art. 49 GDPR:** "1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; the transfer is necessary for important reasons of public interest; the transfer is necessary for the establishment, exercise or defence of legal claims; the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any

*to standard agreements or internationally recognized principles which, pending the adoption of adequacy decisions, in any case offer the interested parties guarantees regarding compliance of fundamental rights and guarantees regarding the protection of personal data (note 15 July 2019)”.*

2. In this year's annual report there was an interview with MAECI with reference to UNHCR ( United Nations High Commissioner for Refugees): *“Another case concerned a request came from the Ministry of the Interior regarding a clause regarding the protection of personal data included in the scheme of the Asylum, Migration and Integration Fund Grant Agreement (FAMI), to be signed with UNHCR, in relation to the transfers of personal data necessary for the management of a project proposal in the field of asylum and resettlement of third-country nationals, to be co-financed with FAMI resources. On this occasion - having recalled the aforementioned regulatory fra-*

---

person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case. Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

2. A transfer pursuant to point (g) of the first subparagraph of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

3. Points (a), (b) and (c) of the first subparagraph of paragraph 1 and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

4. The public interest referred to in point (d) of the first subparagraph of paragraph 1 shall be recognised in Union law or in the law of the Member State to which the controller is subject.

5. In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

6. The controller or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of paragraph 1 of this Article in the records referred to in Article 30”.

**Art. 50 GDPR:** *“In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to: develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data; provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms; engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data; promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries”.*

*mework - the Ministry was also invited to evaluate the use of the hypothesis of derogation, and in particular that for important reasons of public interest (Article 49, paragraph 1, letter d), recalling that the existence of an international agreement or convention establishing a specific objective, to be encouraged through international cooperation, can be an indicator for the purpose of assessing the existence of a public interest, provided that the European Union or the Member States have signed this agreement or convention, referring for the assessment of these conditions to the guidelines of the Committee 2/2018 cited above (note July 26, 2021)”.*

3. Regarding FATCA, data protection rules should play a significant role in taxpayers protection in FATCA. Thanks to the improvements that the GDPR has made in comparison to the Data Protection Directive, the protection that the EU provides for taxpayers via the principle of proportionality should be complied with the FATCA procedures, including data collection, data transfer and data retention.

However, it is possible to find a legal basis for the transfer of data to a third countries in Article 49 of GDPR (“*Derogations for specific situations*”), if one of the conditions listed therein is met: that the interested party has explicitly given his specific and informed consent, that occasional transfer is necessary for the execution of a contract between the data subject and the data controller or between the latter and another natural or legal person, for important reasons of public interest, without looking at the nature of the organization, if it is necessary to exercise a right in court or to protect the vital interests of the data subject who is physically or legally incapable of giving his consent.

In conclusion, data transfer under FATCA to the U.S. requires an adequate level of protection through substantial provisions in IGAs, using the SCCs as said before and, more generally, through an adequacy assessment of US law.

The EDPB, in his Statement on “*International agreements including transfers*”, dated 13 April 2021, invites the Member States “*to assess and, where necessary, review their international agreements that involve international transfers of personal data, such as those relating to taxation (e.g. to the automatic exchange of personal data for tax purposes), social security, mutual legal assistance, police cooperation, etc. which were concluded prior to 24 May 2016 (for the agreements relevant to the GDPR) or 6 May 2016 (for the agreements relevant to the LED)*”.

The EDPB also recommends “*that Member States take into account for this review [...], the relevant EDPB guidelines applicable to international transfers [...]*”, in particular, the EDPB issued Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for “*transfers of personal data between EEA and non-EEA public authorities and bodies*”, adopted on 15 December 2020, and Recommendations 01/2020 on “*measures that sup-*

*plement transfer tools to ensure compliance with the EU level of protection of personal data*", adopted on 18 June 2021, as said before.

Since 2019, with his Statement on "*the US Foreign Account Tax Compliance Act (FATCA)*", the EDPB has ensured to "*review the existing data protection safeguards under the legislation authorising the transfer of personal data to the US IRS for the purposes of the US Foreign Account Tax Compliance Act*", thus working on the preparation of guidelines on some of the tools provided for by Article 46 of the GDPR. In December 2021 about subject rights Italian Supervisory issued advise about dtraft Economy that set up categories and puroposes of data's treatments, in order to takle tax evasion. In this field subjects rights are limited according to budget law 2020.

4. CONSOB National Commission for corporation and market change. Italian Supervisory has approved administrative agreement to transfer personal data among financial authorities in European economic space and outside Europe. This agreement has been the result of long discussion between ESMA (European Securities and markets Authority) and IOSCO (International Organization of Securities Commissions).

5. Another example before GDPR is WADA (World Antidoping Agency): the questions about data of doping has been a matter under attention of European Committee and there was a opinion by WP29.

By this examples we can say that there are some important principles in agreement to transfer personal data: first risch approach, subiect's intervention, the person concerned must be able to intervene at all stages of the procedure about personal data, techniques of anomization, obfuscation and encryption, hourly back-ups, hashing to guarantee an excellent security level, escape clause, time limit for data retention, accountability, privacy by design and default, human loop. This is the base, core of subiects rights to guardianiship of human rights.

Real challenge is Artificial Intelligence and alghoritms in personal data processing: no opacity and right to explanation digital due process are pivotal tools in order to create a trustworthy legal system.