ANNEX:

ARTICLE-BY-ARTICLE ANALYSIS

of the EU-US Umbrella Data Protection Agreement

[TEXT OF THE AGREEMENT IN **BOLD**; COMMENTS ARE IN ORDINARY TYPE]

PREAMBLE:

Mindful **that the United States: and the European Union are committed to ensuring a high level of protection of personal information exchanged in the context of the prevention, investigation, detection, and prosecution of criminal offenses, including terrorism;**

Intending **to establish a lasting legal framework to facilitate the exchange of information, which is critical to prevent, investigate, detect and prosecute criminal offenses, including terrorism, as a means of protecting their respective democratic societies and common values;**

Intending, **in particular, to provide standards of protection for exchanges of personal information on the basis of both existing and future agreements between the US and the EU and its Member States, in the field of preventing, investigating, detecting, and prosecuting criminal offenses, including terrorism;**

Recognizing **that certain existing agreements between the Parties concerning the processing of personal information establish that those agreements provide an adequate level of data protection within the scope of those agreements, the Parties affirm that this Agreement should not be construed to alter, condition, or otherwise derogate from those agreements; noting however, that the obligations established by Article 19 of this Agreement on judicial redress would apply with respect to all transfers that fall within the scope of this Agreement, and that this is without prejudice to any future review or modification of such agreements pursuant to their terms.**

Acknowledging **both Parties' longstanding traditions of respect for individual privacy including as reflected in the Principles on Privacy and Personal Data Protection for Law Enforcement Purposes elaborated by the EU-US High Level Contact Group on Information Sharing and Privacy and Personal Data Protection, the Charter of Fundamental Rights of the European Union and applicable EU laws, the United States Constitution and applicable US laws, and the Fair Information Practice Principles of the Organization for Economic Cooperation and Development;**

Analysis: The Parties ignore that the human rights issues raised by data exchanges in a law enforcement context extend well beyond privacy to protection against arbitrary arrest and detention, treatment in detention, fair trial, freedom of movement, etc.. More specifically, the parties ignore the fundamental principle of universality of human rights: those rights should accrue to “everyone”, irrespective of nationality or place of residence. By doing so, the parties allow continued, unjustifiable discrimination between different categories of individuals – “US persons”, EU and US nationals and people who are neither EU nor US nationals – under US law, in breach of international human rights treaties, including the International Covenant on Civil and Political Rights to which the USA are a party. The above recital thus ignores the fact that US law offers much less protection than EU law in respect of the collection and use of personal data, and in many cases affords little or no protection to non-EU citizens, and that this will remain so in many respects even after

the entering into force of this Agreement (as noted in our specific analyses of the Agreement's articles, below).

and

Recognizing **the principles of proportionality and necessity, and relevance and reasonableness, as implemented by the Parties in their respective legal frameworks;**

Analysis: Note the "in their respective legal frameworks". The US view of what is "necessary", "proportionate", "relevant" and "reasonable" in a particular case will thus apply to any data transferred to the USA – even if that view is more permissive of than the EU one, as it generally is, and in particular in relation to third-party disclosures. For instance, "reasonableness" in the US might entail the "need to know" principle.

THE UNITED STATES OF AMERICA AND THE EUROPEAN UNION HAVE AGREED AS FOLLOWS:

Article 1: Purpose of the Agreement

1. The purpose of this Agreement is to ensure a high level of protection of personal information and enhance cooperation between the United States and the European Union and its Member States, in relation to the prevention, investigation, detection or prosecution of criminal offenses, including terrorism.

Analysis: Note the phrase "high level" – which is not the same as stipulating that the level of protection is equivalent to the protection of persons' fundamental rights pursuant to the standards of the EU Charter of Fundamental Rights.

2. For this purpose, this Agreement establishes the framework for the protection of personal information when transferred between the United States, on the one hand, and the European Union or its Member States, on the other.

3. This Agreement in and of itself shall not be the legal basis for any transfers of personal information. A legal basis for such transfers shall always be required.

Analysis: The "legal basis for the transfers" will generally be either a bilateral MLAT between an EU Member State and the USA, and/or the general EU-US MLAT Agreement of 2003.[1] But this latter treaty in particular is dubious in terms of data protection. Note in particular the Explanatory Note on the EU-US MLAT which the Note expressly states was "agreed between the Contracting Parties" (i.e., the EU and the USA), which means it is part and parcel of the binding treaty (and itself therefore also binding) and which says, *inter alia*, in relation to Article 9:

> Article 9(2)(b) is meant to ensure that refusal of assistance on data protection grounds may be invoked only in exceptional cases. Such a situation could arise if, upon balancing the important interests involved in the particular case (on the one hand, public interests, including the sound administration of justice and, on the other hand, privacy interests), furnishing the specific data sought by the requesting State would raise difficulties so fundamental as to be considered by the requested State to fall within the essential interests grounds for refusal. **A broad, categorical, or systematic application of data protection principles by the requested State to refuse**

[1] Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 181, 19.7.2003, p. 34–42.

> **cooperation is therefore precluded. Thus, the fact the requesting and requested States have different systems of protecting the privacy of data (such as that the requesting State does not have the equivalent of a specialised data protection authority) or have different means of protecting personal data (such as that the requesting State uses means other than the process of deletion to protect the privacy or the accuracy of the personal data received by law enforcement authorities), may as such not be imposed as additional conditions under Article 9(2a).** (emphasis added)

Note that this prohibition of "generic data protection restrictions" is repeated in the Umbrella Agreement in Article 6(3): see the analyses of that article (and of Article 5(3) to which Article 6(3) refers).

Article 2: Definitions

For purposes of this Agreement:

1. **"Personal information" means information relating to an identified or identifiable natural person. An identifiable person is a person who can be identified, directly or indirectly, by reference to, in particular, an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.**

Analysis: This definition of "personal information" is effectively identical to the definition of "personal data" in Article 2(a) of the 1995 DP Directive.

2. **"Processing of personal information" means any operation or set of operations involving collection, maintenance, use, alteration, organization or structuring, disclosure or dissemination, or disposition.**

Analysis: This definition of "processing of personal information" largely corresponds to the definition of "processing of personal data" in Article 2(b) of the 1995 DP Directive – but not entirely, as indicated in bold below:

> (b) 'processing of personal data'('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, **recording**, organization, **storage**, adaptation or alteration, **retrieval**, **consultation**, use, disclosure by transmission, dissemination or **otherwise making available**, **alignment or combination**, **blocking**, erasure or destruction;

The definition in the Umbrella Agreement thus omits some significant acts that can be performed upon personal data, i.e.: "recording", "storage", "retrieval", "consultation", "alignment or combination" (i.e., "matching", which is important in relation to the creation of "profiles"), and "blocking"; and the Agreement also (unlike the Directive) does not spell out that "making [personal data] available" in some way other than by "transmission or dissemination" still constitutes a "disclosure" of the data. The very fact that the above specifics are omitted from the Agreement is suspicious: *it must be assumed that these omitted actions are expressly intended to be excluded from the Agreement*.

NB: Some US and UK authorities (as well as some US business leaders) have recently suggested that personal data are only "collected" when they are accessed by a human person, i.e., that the automated "hoovering up" of (communications) data in bulk (in particular from the undersea cables) does not (yet) constitute "collecting" those data. This

may be relevant here too. According to the CJEU's recent *Schrems* judgment, EU data protection standards should also apply whenever the data is collected and stored, not just when it is accessed.

3. "Parties" means the European Union and the United States of America.

4. "Member State" means a Member State of the European Union.

5. "Competent Authority" means, for the United States, a US national law enforcement authority responsible for the prevention, investigation, detection or prosecution of criminal offenses, including terrorism and, for the European Union, an authority of the European Union, and an authority of a Member State, responsible for the prevention, investigation, detection or prosecution of criminal offenses, including terrorism.

Analysis: This must be read together with Article 3(2), which totally excludes "transfers or other forms of cooperation between the authorities of the Member States and of the United States other than those referred to in Article 2(5), responsible for safeguarding national security", from the scope of the Umbrella Agreement.

That is a seriously problematic matter, because increasingly law enforcement authorities (LEAs) are becoming inseparably intertwined with national security agencies (NSAs), in particular in relation to terrorism, more in particular in relation to the "prevention" of terrorist offences. Traditionally, when terrorism was regarded as a national security issue, the national security (or "intelligence") agencies were responsible for the general gathering of information on them (and infiltrating them, etc.). The ordinary law enforcement agencies – the normal civilian police – only became involved if there was some indication of an actual plot to commit a specific offence – while they of course did not have to sit and wait until a bomb was actually primed or had already exploded, they would not generally be involved in more general intelligence gathering (although special agencies with the LEAs, such as the Special Branch in the UK, did and do engage into these more secret service-type activities). If the distinction was always rather slippery, this has become worse in modern times, with the increased threat of global terrorism (although it also happened earlier, in relation to local or regional threats, such as the BR, RAF, IRA and ETA campaigns of the 1970s – 90s).

But now, increasingly, the roles of LEAs and NSAs are no longer even formally treated as distinct. This applies in particular to the US FBI: as noted in the *Issue Paper* on The Rule of Law on the Internet and in the wider digital world of the Council of Europe Commissioner for Human Rights:[2]

> A page on the FBI website, "Addressing threats to the nation's cybersecurity", expressly notes that the FBI is charged with protecting the USA's national security and with being the nation's principal law-enforcement agency, adding that "These roles are complementary, as threats to the nation's cybersecurity can emanate from nation-states, terrorist organizations, and transnational criminal enterprises; with the lines between sometimes blurred." See: www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity.

[2] The rule of law on the Internet and in the wider digital world, *Issue Paper* published by the Council of Europe Commissioner for Human Rights, CommDH/IssuePaper(2014)1, 08 December 2014, prepared by Douwe Korff, footnote 6, on p. 29. The *Issue Paper* is available at: https://wcd.coe.int/ViewDoc.jsp?Ref=CommDH/IssuePaper(2014)1&Language=lanAll

> [Indeed, the FBI] has changed an FBI Fact Sheet to describe its "primary function" as no longer "law enforcement", but now "national security". See *The Cable*, 5 January 2014: http://thecable.foreignpolicy.com/posts/2014/01/05/fbi_drops_law_enforcement_as_primary_mission#sthash.4DrWhlRV.dpbs.
>
> For the dangers inherent in such blurring of the lines, see: www.foreignpolicy.com/articles/2013/11/21/the_obscure_fbi_team_that_does_the_nsa_dirty_work.

This question of which organisations, in particular but not only in the USA, can be considered to be "competent authorities" within the meaning of Article 2(5) of the Umbrella Agreement is therefore far from clear. Is the FBI? This question relates closely to the issue of onward transfers: see the analysis of Article 7, below.

Article 3: Scope

1. This Agreement shall apply to personal information transferred between the Competent Authorities of one Party and the Competent Authorities of the other Party, or otherwise transferred in accordance with an agreement concluded between the United States and the European Union or its Member States, for the prevention, detection, investigation and prosecution of criminal offences, including terrorism.

Analysis: The above means that the Umbrella Agreement applies not only to specifically LEA-related agreements such as MLATs (including the EU-US MLAT of 2003), but also to transfers of personal data from the EU to the USA under any other EU-US agreements aimed (*inter alia*) at the prevention, detection, investigation and prosecution of criminal offences, including terrorism – such as the latest (2012) EU-US PNR Agreement.[3] However, the hierarchical status of the Umbrella Agreement's data protection provisions in relation to those in such other agreements is unclear: those in the Umbrella Agreement "supplement" those other ones, but it is unclear which ones prevail in case of a conflict (see the analysis of Article 5(1), below).

2. This Agreement does not affect, and is without prejudice to, transfers or other forms of cooperation between the authorities of the Member States and of the United States other than those referred to in Article 2(5), responsible for safeguarding national security.

Analysis: See the analysis of Article 2(5), above. This means that the Umbrella Agreement does not in any way limit the transfer of personal data from any EU Member State NSA to any US NSA (or any other cooperation between such EU Member State and US agencies). In one way, this reflects the seemingly total exclusion of EU competence over any matter relating to any Member States' activities relating to "national security" (Art. 4(2) TEU) – but which is not quite as absolute as some Member States would like to pretend.[4]

---

[3] On the EU-US PNR Agreements (of which there have been three), see: Douwe Korff & Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards, draft report for the Council of Europe Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-DP), presented to the 32nd Plenary of the Committee in Strasbourg (France) on 1 July 2015, currently being finalised, section IV.i – EU-Third Country PNR Agreements, p. 67ff.

[4] For a discussion of this exclusion and its limits, see Douwe Korff, Surveillance and the EU general data protection regulation: possibilities, limits and obstacles, *Datenschutz Nachrichten* 4/2013 (December 2013),

But it touches on the very difficult question of data disclosures from entities that are subject to EU law (including the Charter, and the draft Law Enforcement Data Protection Directive) – i.e., in particular, Member States' LEAs – to entities even within the same Member State such as their NSAs, that are (at least to a large extent, but in the view of those already-mentioned Member States, wholly) outside of the scope of Union law (and thus even outside of the Charter); and to the possible further passing on of the thus internally-disclosed data to NSAs in non-EU countries, including the USA. For instance: if data are disclosed, under EU rules, by an Italian LEA to a Dutch LEA, and if under Dutch law that Dutch LEA is allowed to share the data with a Dutch NSA, does the above provision mean that the Umbrella Agreement is totally inapplicable to the further passing on of those data from the Dutch NSA to a US NSA (such as the actual US NSA)?[5] If EU Member States' LEAs are allowed to share the data they receive from other Member States' LEAs with their own NSAs, in particular in relation to terrorism, and if those NSAs are then not prohibited from passing the data on to the US NSAs (or indeed to anyone), that clearly opens up a massive hole in the Umbrella Agreement: the umbrella then seriously leaks.

To some extent, this depends on the "compatible [further] processing" rules in the Umbrella Agreement and in the rules under which the data were disclosed to the MS in question. See the analysis of Article 6(2), below.

Article 4: Non-Discrimination

Each Party shall comply with its obligations under this Agreement for the purpose of protecting personal information of its own nationals and the other Party's nationals regardless of their nationality, and without arbitrary and unjustifiable discrimination.

Analysis: Note that this emphatically does **not** say that each party shall provide equal protection of any personal data processed by its LEAs relating to, on the one hand, its own nationals, and on the other, the nationals of the other party. First of all, the obligation to treat nationals of the EU (= EU citizens) and US nationals the same only applies in relation to "[the parties'] obligations under this Agreement". In respect of anything that is not covered by the agreement, the parties can make (or retain) as many distinctions as they like.

Secondly, the principle of equality only applies to *nationals* of the EU and the USA. Data on (say) an Australian or Afghan resident in the EU, or flying to or from the EU (transferred under the PNR treaty)– or on, say, any Syrian refugees given asylum in the EU but not citizenship – would not appear to be protected. At most, they (and their data) should not be subjected to "arbitrary and unjustifiable discrimination" – which is a rather different test from equal treatment.

In sum: The Umbrella Agreement does not protect EU citizens, and certainly also not any non-EU national whose data are sent by an EU authority to the USA, from discriminatory treatment.

---

pp. 150-4 (not available online) and Korff's expert opinion to the German *Bundestag* Committee of Inquiry into the Snowden revelations, section B.2(e), at pp. 34-39, available at: https://www.bundestag.de/blob/282874/8f5bae2c8f01cdabd37c746f98509253/mat_a_sv-4-3_korff-pdf-data.pdf

[5] The example would be even more to the point if in stead of "Dutch", one chooses "UK". However, the UK will not be automatically be bound by the Agreement; it will only be so bound if it declares that it agrees to do so: see Article 27. It will be important to check if, if and when the UK were to sign up to the Agreement, it will enter any reservations or declarations to the Agreement, in particular in relation to the status of its NSAs.

As noted in the analysis of Article 19, below, this unequal treatment and discrimination is carried through to, and further reinforced, in connection with judicial redress against violations of the Agreement. It is in clear breach of the Charter (and European and international human rights- and data protection law, including the ECHR). It could only be fixed by amending Article 4 to reflect the fundamental international human rights principle set out in Article 2(1) of the International Covenant on Civil and Political Rights, to read:

> Each Party shall implement this Agreement, and accord all the rights and guarantees provided for by this Agreement to everyone, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status, including nationality or residence status.

Article 5: Effect of the Agreement

1. This Agreement supplements, as appropriate, but does not replace, provisions regarding the protection of personal information in international agreements between the Parties, or the United States and Member States that address matters within the scope of this Agreement.

Analysis: This provision does little to clarify the relationship between the Umbrella Agreement and other agreements between the EU and the USA (including the EU-US PNR Agreement and the EU-US MLAT of 2003), and between the Umbrella Agreement and agreements between the USA and any MS (including MLATs between them). It says that the Umbrella Agreement "supplements ... but does not replace" any data protection rules in those other treaties. That is fine if those other treaties do not contain any data protection provisions, or if any such provisions do not cover any of the matters covered by the Umbrella Agreement. But what if there are competing, or even conflicting rules in the instruments? Do the most data protection-friendly rules apply? This is not made clear. It should be.

2. The Parties shall take all necessary measures to implement this Agreement, including, in particular, their respective obligations regarding access, rectification and administrative and judicial redress for individuals provided herein. The protections and remedies set forth in this Agreement shall benefit individuals and entities in the manner implemented in the applicable domestic laws of each Party. For the United States, its obligations shall apply in a manner consistent with its fundamental principles of federalism.

Analysis: The stipulation that "*The protections and remedies set forth in this Agreement shall benefit individuals and entities in the manner implemented in the applicable domestic laws of each Party*" is problematic to the extent that US law in several respects severely limits the scope of US "protections and remedies".

First of all, as also noted in the quote, below, the Privacy Act contains sweeping exemptions from basic privacy/data protection principles that go way beyond what is compatible with fundamental EU (and constitutional Member State!) principles – so even if EU citizens were to be given the same "protections and remedies" as US nationals, those would still fall far short of what Union law – including the Charter – and Member State law – including Member States' constitutions! – require.

Secondly, to the extent that the reference to "protections and remedies" relates to the Judicial Redress Act (the adoption of which is a *sine qua non* for the entering into force of the Umbrella Agreement: see the main Note]), this too is not nearly sufficient from an EU point of view. To quote Francesca Bignami of George Washington University:[6]

> By its very terms, it [the Judicial Redress Act]is it not designed to create absolute equality of treatment between US persons and EU citizens: it excludes damages liability for adverse determinations based on inaccurate or otherwise unlawful personal data and it excludes damages liability for any "failure to hew to the terms of the Act," with the exception of unlawful disclosure.
>
> [What is more, t]he Act includes all the limitations applicable to US persons, which are extensive in the law enforcement arena. Since law enforcement records are routinely exempted from the Privacy Act, if the exemption is claimed, the one type of law suit that would remain for EU citizens is a civil suit for intentional or willful disclosures that caused the plaintiff actual damages.
>
> Unlike US persons, the Act says that the remedies provided are exclusive. Therefore it might preempt other statutory law (e.g. Federal Tort Claims Act) or common law claims, for instance tort claims or contract claims against a government contractor or invasion of privacy tort claims, or perhaps even arbitral remedies available against private and government entities.

This is quite simply unacceptable, as further discussed in the analysis of Article 19.

3. By giving effect to paragraph 2, the processing of personal information by the United States, or the European Union and its Member States, with respect to matters falling within the scope of this Agreement, shall be deemed to comply with their respective data protection legislation restricting or conditioning international transfers of personal information, and no further authorization under such legislation shall be required.

Analysis: *Das ist des Pudel's Kern*, so to speak (here is the core issue, for those not familiar with Goethe's Faust in the original German ☺). Once the USA has "given effect" to the – as just noted, from a European Union perspective, seriously deficient – "protections and remedies" in the Umbrella Agreement, neither the EU, nor any EU law enforcement institution, nor any Member State, will be allowed to restrict the transfers of personal data covered by the Agreement, or impose conditions on such transfers, on the basis of any EU- or national law that might otherwise have allowed or required the imposition of such restrictions or conditions. Rather, the USA will be "deemed" to have met any conditions in such laws.

First of all, this would appear to be in clear breach of the Treaties and the Charter. In its recent judgment in *Schrems*, the CJEU has made clear that the Charter requires that national data protection authorities must retain authority to assess whether transfers of personal data are consistent with EU law, without being faced with a presumption of compatibility (such as the Commission tried to impose under the "Safe Harbor" Agreement); and must be able to refer question of such compatibility of relevant instruments with the Charter to the Court. The inclusion of a similar – indeed if anything stronger and even more irrebuttable –

6 [ADD LINK]

presumption of compatibility in the Umbrella Agreement is *prima facie* in clear breach of this principle.

As important, it is highly doubtful whether this is compatible with at least some Member States' constitutions, in particular the German one. In its *Solange* decisions, the Karlsruhe Court has always retained for itself the right to be the ultimate judge to decide whether any EU law is compatible with the fundamental rights requirements of the German Constitution. The German Constitutional Court has accepted that in practice the Luxembourg Court will (almost?) always ensure that any EU rules that might violate the basic German ones would be either declared invalid under EU law (including the Charter) or interpreted in a way that meets the German constitutional minimum requirements. However, the Karlsruhe Court has never abandoned the principle that *in extremis* it, and not Luxembourg, would still have the final say. It is unlikely that the German Constitutional Court will accept the implication of this Article 5(3), that German data protection law – which is strongly supported by the German Constitution and by the Constitutional Court – can no longer be invoked as a basis for imposing "restrictions or conditions" on the transfer of (often highly sensitive) personal data by German law enforcement agencies to their counterparts in the USA, and that neither the German data protection authorities, nor the Luxembourg or Karlsruhe court would have any further say in the matter.

Similarly, the European Court of Human Rights has on occasion found that the scope of national courts' review of privacy issues had been unduly restricted, and that that violated the Convention. In that light, it is highly likely that that court too would reject the exclusion of the competence of the courts of the parties to the ECHR in respect of the Umbrella Agreement.

Of course, these courts could decline to rule on this issue *in abstracto* and effectively tell individuals to raise it only as and when there might be a conflict in a particular case. But this "deeming" provision would still continue to acts as a "ticking bomb" under the Agreement. It could for instance quite quickly be challenged in a concrete case by, say, a Syrian refugee settled in Germany: cf. the analysis of Article 4, above. In any case, the Strasbourg court has, since its *Klass* judgment repeatedly accepted applications that effectively challenged a law relating to data processing by law enforcement and/or national security authorities, without requiring that individuals prove that they were actually affected by the law in question.

Article 6: Purpose and Use Limitations

1. The transfer of personal information shall be for specific purposes authorized by the legal basis for the transfer as set forth in Article 1.

Analysis: It is important to note that Article 1(3) stresses that the Agreement itself does not constitute a "legal basis" for a transfer: the legal basis has to be found in another agreement (e.g., the EU-US MLAT, or a US-EU MS MLAT, or indeed as we have seen the EU-US PNR Agreement). But once such a legal basis has been determined: (i) the processing of the personal data must comply with the Agreement, and (ii) no "restrictions or conditions" can be imposed on the transfer beyond the requirements of the Agreement. But *re* (i), see my comments on Article 5(1), and *re* (ii), see my comments on Article 5(3), above.

2. The further processing of personal information by a Party shall not be incompatible with the purposes for which it was transferred. Compatible processing includes processing pursuant to the terms of existing international agreements and written

international frameworks for the prevention, detection, investigation or prosecution of serious crimes. All such processing of personal information by other national law enforcement, regulatory or administrative authorities shall respect the other provisions of this Agreement.

Analysis: This is a very tricky provision. In essence it says that once data are transferred under any treaty (mainly any MLAT, including the EU-US MLAT and any US-EU MS MLAT), the data can also be used "pursuant to the terms of [*any other*] existing international agreements and written international frameworks for the prevention, detection, investigation or prosecution of serious crimes" and – crucially – by "[*any*] *other* national law enforcement, regulatory or administrative authorities [of the receiving state]".

The words "international frameworks for the prevention, detection, investigation or prosecution of serious crimes" could relate to multilateral international treaties such as the Cybercrime Convention, or the Council of Europe European Convention on Mutual Assistance in Criminal Matters. But they, and the words "existing international agreements", can also be given a wider reading to cover essentially any "international agreement" or "written international framework" entered into or created (also) "for the prevention [etc.] of serious crimes." That would seem to me to be very open-ended – especially in view of the reference to authorities other than law enforcement ones. Indeed, it could be read as covering the sharing of data in shadowy "intelligence clubs" such as those listed in the Note to which this is an Annex,[7] since (as discussed in the Note) the relevant "national security" or "intelligence" agencies are increasingly involved also in the prevention etc. of (serious) crime and terrorism.

Also seriously worrying is the use of the word "including" in the second sentence. This means that State Parties can claim that some other "further processing" for some other, not-defined purpose is also "compatible" with the purposes for which the data were originally transferred – especially since "disclosure" is expressly included in the definition of "processing". For instance, the USA could claim that the disclosure of data obtained by one of its law enforcement agencies from an LEA in an EU Member State, for the purpose of investigating a specific (confirmed or suspected) terrorist offence, by that US LEA, to one of the US national security agencies, for general counter-terrorism purposes (including anti-terrorist data mining and profiling: see the analysis of Article 15, below), is "compatible" with the original purpose of the transfer. In fact, as noted in my comments under Article 2(5), above, the FBI defines itself as both a law enforcement agency *and* a national security agency – which suggests that such disclosures are regarded as inherently compatible. In the UK, GCHQ is similarly increasingly involved in what used to be law enforcement areas.

It will be important to clarify that neither data disclosures allowed under the terms of treaties between EU Member States and the USA on national security cooperation, nor the (further) disclosure of the data within the USA to the US national security authorities are to be deemed to be "compatible" ("not incompatible") with the Umbrella Agreement, simply because they are done "pursuant to the terms of existing international agreements". This should apply *a fortiori* to any secret (or partially secret) treaties of such a kind[8] – which by

[7] E.g., the "Brenner Club"; the "Club of Berne"; the "G6 Group"; "Megatonne"; the "Kilowatt Group"; etc.: see pp. 7-8 of the Note.

[8] Apparently, in the area of crossborder cooperation on "national security" issues, secret treaties are the norm rather than the exception; and even if the basic treaties are published, they often contain unknown

their very nature do not constitute "law" in the sense of the Charter or the ECHR and can therefore never be a basis for any interference with fundamental rights.

At the very least, the state that originally transferred the data should be able to stipulate whether the data can, or may not, be further shared or transferred in such a way, with or to such other agencies.

See also the analysis of Article 3(2), above.

3. This Article shall not prejudice the ability of the transferring Competent Authority to impose additional conditions in a specific case to the extent the applicable legal framework for transfer permits it to do so. Such conditions shall not include generic data protection conditions, that is, conditions imposed that are unrelated to the specific facts of the case. If the information is subject to conditions, the receiving Competent Authority shall comply with them. The Competent Authority providing the information may also require the recipient to give information on the use made of the transferred information.

Analysis: This provision reflects Article 9 of the EU-US MLAT, as interpreted in the Explanatory Note on that Agreement, quoted in the analysis of Article 1(3), above. It allows for the imposition, by a state transferring the data, of case-specific conditions (such as a specific retention period, or a restriction on further transfer of specific data) – but it expressly bars EU Member States (or the EU or any of its agencies) from imposing "generic data protection conditions". Since such "generic conditions" might well flow from the Charter (in relation to the EU and EU institutions), or from a Member State's constitutional requirements, this prohibition can again raise serious issues in relation to EU and Member States' domestic constitutional law, of the kind already discussed in the analysis of Article 5(3), above.

It would appear, for instance, that an EU Member State may not impose the "generic condition" for transfers involving or including data on non-nationals of that Member State (such as refugees settled in that state but not granted citizenship), that those data should be protected equally as are data on the Member States' nationals (cf. the analysis of Article 4, above). But transferring the data to the USA without such a condition – i.e., allowing discrimination in this regard, by the US receiving authorities, between [data on] the Member State's nationals and residents that are not citizens – may well be in violation of the Member State's constitution.

4. Where the United States, on the one hand, and the European Union or a Member State on the other, conclude an agreement on the transfer of personal information other than in relation to specific cases, investigations or prosecutions, the specified purposes for which the information is transferred and processed shall be further set forth in that agreement.

---

secret annexes or separate, secret agreements on their application and interpretation. Where, in rare cases, the veil of secrecy has been partially lifted, it has been shown that the relevant treaties also and especially deal with the making available and/or sharing of data – including especially communications data. See, for a revealing insight into the national security treaties between Germany and the Western Allies and former Allies: Joseph Foschepoth, Überwachtes Deutschland, 3rd ed., 2013.

5. The Parties shall ensure under their respective laws that personal information is processed in a manner that is directly relevant to and not excessive or overbroad in relation to the purposes of such processing.

Analysis: The first of these two provisions (para. 4) is not about MLATs (EU-US and US-EU MSs): those deal with transfers of data relating to "specific cases, investigations or prosecutions." So this provision presumably applies to agreements on the suspicion-less provision of data in bulk, as under the EU-US PNR Agreement, etc.. The text of this provision, and the next one (para. 5) suggests that such agreements are fine as long as they (i) specific the purpose*s* (note the plural) of the (bulk) transfers, and (ii) *process* the data "in a *manner* that is directly relevant to and not excessive or overbroad in relation to the purposes of such processing". But *processing* the data a "*manner*" that is "directly relevant to and not excessive or overbroad in relation to the purposes of such processing" is not the same as the data themselves having to be "directly relevant to and not excessive or overbroad in relation to the purposes of such processing". Since much of the data contained in PNRs are (i) "irrelevant and excessive" for normal law enforcement purposes, and (ii) are used for profiling purposes,[9] one may wonder if this odd text is an attempt to allow for the transfer of "irrelevant, excessive and overbroad" data, as long as they are not *used* in an "irrelevant, excessive and overbroad" *manner*? (With the US authorities of course arguing that their data analyses and profiling operations are not "irrelevant, excessive and overbroad".) This would be incompatible with the EU Charter as interpreted by the CJEU in *Schrems*, which held that mass surveillance by third countries is in principle incompatible with the very essence of the right to privacy.

Article 7: Onward Transfer

1. Where a Competent Authority of one Party has transferred personal information relating to a specific case to a Competent Authority of the other Party, that information may be transferred to a State not bound by the present Agreement or international body only where the prior consent of the Competent Authority originally sending that information has been obtained.

Analysis: It is a concern here that the "Competent Authority" in question is an LEA, and the first concern of an LEA is to be helpful to other LEAs, rather than ensuring high levels of data protection for the benefit of people who have already "come to the attention" of the authorities. It would be better – and more compatible with the Charter – if the "consent" were to be given by the data protection authority charged with ensuring compliance with data protection law by the LEA concerned (which is often a specialised DPA for LEAs).[10] And it should be spelled out, in unambiguous terms, that consent should be withheld if the transfer could result in a violation of the country's (or the EU's) data protection laws or –principles.

Moreover, as a more general principle, no data – and certainly no personal data – should ever be allowed to be passed on to LEAs in countries not party to the Agreement, if such

[9] See Douwe Korff and Marie Georges, o.c. (footnote 3, above).

[10] This is not the place to discuss general issues of data protection oversight over the processing of personal data by LEAs and EU law. Suffice it to note that although under the Charter there should always be an "independent authority" competent to exercise control over any such processing (Art. 8(3) of the Charter), in a number of Member States (including France) the competences and status of the relevant authorities are still a matter for discussion.

transfers could result in serious human rights violations. That is binding international law if the transfer of the data could result in torture.

But data originating from EU LEAs should also never be made available to third countries in cases in which this could result in persecution or wrongful arrest or detention of a person, or in unfair trials – or in actions such as drone killings. We have seen the serious negative human rights implications of Western States' cooperation with dictatorships such as Ghadaffi's in the "fight against terrorism", as well as names given to the Syrian secret service by Member States' intelligence agencies. This Agreement should emphatically not facilitate that. On the contrary, a general human rights clause should emphasise this principle. Such a clause is missing. It is crucial that it be added.

2. When granting its consent to a transfer under paragraph 1, the Competent Authority originally transferring the information shall take due account of all relevant factors, including the seriousness of the offence, the purpose for which the data is initially transferred and whether the State not bound by the present Agreement or international body in question ensures an appropriate level of protection of personal information. It may also subject the transfer to specific conditions.

Analysis: This strongly reinforces the above concern: not only is it again the "Competent Authority", i.e., an LEA, that is supposed to weigh these factors – worse, the factors and the way they are listed clearly suggests that data protection requirements can be overridden if the offence in question is "serious" enough. The reference to the third state "ensur[ing] an appropriate level of protection of personal information" is, if anything, out of place here. If the third state does indeed ensure such a level of protection *in relation to the processing envisaged, i.e., by the recipient LEA*, and if that has been formally held to be the case by the EU, then the situation is fundamentally different; in such cases, cooperation should in principle be fine. But the "trading off" of data protection against the interests of international LEA cooperation is dangerous. At the very least, this requires a much more detailed set of provisions. And again, these matters should not be left to the sending LEA to weigh, but should be in the hands of the relevant (i.e., LEA sector-specific) DPA. There should also be full transparency about the way this provision is applied in practice: see the analysis of Article 20, below.

3. Where the United States, on the one hand, and the European Union or a Member State on the other, conclude an agreement on the transfer of personal information other than in relation to specific cases, investigations or prosecutions, the onward transfer of personal information may only take place in accordance with specific conditions set forth in the agreement that provide due justification for the onward transfer. The agreement shall also provide for appropriate information mechanisms between the Competent Authorities.

Analysis: This again relates to the agreements relating to suspicion-less bulk provision of data such as PNR. Of course, these should regulate – and in principle prohibit – onward transfers to states not party to those agreements. If those are allowed, they should be very strictly regulated – we are talking here of massive amounts of data on mostly totally innocent individuals, yet which can be clearly used against them by repressive governments (e.g., if they show travel to certain events, or contacts with certain people or groups).

Just having "appropriate information mechanisms *between the Competent Authorities*" is not nearly enough. Again, at the very least, this requires a much more detailed set of provisions. Again, these matters should not be left to the sending LEA to weigh, but should be in the hands of the relevant (i.e., LEA sector-specific) DPA. The relevant "agreements" should be specific, e.g., as to the precise size of any bulk data, origin of the data, the means to process the data, and the purpose of the agreement . And again, there should be full transparency about the way this provision is applied in practice: see the analysis of Article 20, below.

4. Nothing in this Article shall be construed as affecting any requirement, obligation or practice pursuant to which the prior consent of the Competent Authority originally transferring the information must be obtained before the information is further transferred to a State or body bound by this Agreement, provided that the level of data protection in such State or body shall not be the basis for denying consent for, or imposing conditions on, such transfers.

Analysis: This rather convoluted provision appears to deal with the disclosure of data by an LEA subject to the Umbrella Agreement [LEA A] to an LEA in another country that is also subject to the Agreement [LEA B], and then with the further transfer of those data to yet another LEA subject to the Agreement (in the country of the original recipient LEA or, more likely, in yet another country) [LEA C]. The provision accepts that in some such cases the original disclosing authority [A] may stipulate that the data may not be so further disclosed (by [B] to [C]) without its [A's] prior consent. What those cases are is not spelled out.

Presumably, this applies whenever the instrument providing the legal basis for the transfer (such as an MLAT) contains such a stipulation (or if seeking consent has become the practice between the states concerned). Article 7, para. (4), makes clear that such stipulations in such other treaties are not affected by the Umbrella Agreement – prior consent in the relevant cases will still be required. But it then adds a *caveat*: "provided that the level of data protection in such State or body shall not be the basis for denying consent for, or imposing conditions on, such transfers." In other words, parties to the Umbrella Agreement are no longer allowed to rely on such prior consent stipulations in such other treaties to prevent an onward transfer to "another body bound by [the Umbrella Agreement]", merely because it believes that the level of data protection in the country of the final recipient, [C] (and more specifically, the level of data protection as applied to [C]), is not sufficient.

This raises the same issues as already noted in the analyses of Articles 5(3) and 6(3), above: it would seem that the Umbrella Agreement, here too, tries to bar national data protection authorities or courts, including the CJEU and any EU Member State constitutional court, from prohibiting transfers – also of data on its own citizens or residents – on the basis that the ultimate recipient in another country that is party to the Agreement is not effectively subject to an appropriate level of data protection.

Again, this is unlikely to be acceptable to the legal orders in question, in light of the CJEU ruling in *Schrems*.

Article 8: Maintaining Quality and Integrity of Information

The Parties shall take reasonable steps to ensure that personal information is maintained with such accuracy, relevance, timeliness and completeness as is necessary and appropriate for lawful processing of the information. For this purpose, the Competent Authorities shall have in place procedures, the object of which is to ensure the quality and integrity of personal information, including the following:

(a) the measures referred to in Article 17;

(b) where the transferring Competent Authority becomes aware of significant doubts as to the relevance, timeliness, completeness or accuracy of such personal information or an assessment it has transferred, it shall, where feasible, advise the receiving Competent Authority thereof;

(c) where the receiving Competent Authority becomes aware of significant doubts as to the relevance, timeliness, completeness or accuracy of personal information received from a governmental authority, or of an assessment made by the transferring Competent Authority of the accuracy of information or the reliability of a source, it shall, where feasible, advise the transferring Competent Authority thereof.

Analysis: There are two matters of serious concern here. First of all, there is the use of weasel-words that significantly tone down the requirements of the provision: the states concerned must take "*reasonable steps*" (not even: "*all* reasonable steps" to ensure "*such accuracy*", etc., as is necessary and "*appropriate*"; and they need only inform each other of "*significant doubts*" about such matters, and even then only "*where feasible*". This constrasts quite starkly with the main EC Data Protection Directive which stipulates that:

> **It shall be for the controller to ensure** [*inter alia*] **that** [any personal data processed by or under the authority of the controller are:]
>
> (c) **adequate**, relevant and **not excessive** in relation to the purposes for which they are collected and/or further processed; [as well as]
>
> (d) accurate and, where necessary, kept up to date.
>
> (Article 6(2) and (1)(c) and (d), first sub-sentence, of the 1995 Directive read together, words missing from the Umbrella Agreement highlighted in bold)

Being under a legal obligation to "ensure" that data are adequate, relevant, not excessive, accurate and up to date (the EU test) is rather more than "taking reasonable steps" to ensure "accuracy, relevance, timeliness and completeness", as and when "necessary and appropriate" (presumably, in the eye of the controller). The absence of any reference to a need for the data to be "adequate" and "not excessive" underlines this weakness of the provision in the Umbrella Agreement, all the more so since this relates to the highly sensitive area of exchanges of law enforcement data

But in fact, matters are worse. Article 8 notably omits to spell out what remedial action must be taken if data are identified as (actually or possibly) inaccurate, irrelevant, out of date, or so incomplete as to be potentially misleading. There is nothing in Article 8 of the Umbrella Agreement that says anything on the lines stipulated in the main Data Protection Directive, as follows:

> every reasonable step must be taken [by the controller] to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are **erased or rectified**.
>
> (Article 6(1)(d), second sub-sentence, of the 1995 Directive, emphasis in bold added)

This is a serious omission, especially in the light of the (as explained, binding) Explanatory Note on the EU-US MLAT, already quoted in the analysis of Article 1(3), above, according to which, *inter alia*:

> [The fact that] the requesting State [NB: that would under the Umbrella Agreement be the state receiving the data] uses **means other than the process of deletion to protect the privacy or the accuracy of the personal data** received by law enforcement authorities [may not be invoked by the transferring state as a reason for not transferring the data, or to impose "generic conditions" on the transfer, e.g., that erroneous data be erased].

In this respect, too, the Umbrella Agreement (and for that matter, the EU-US MLAT of 2003) thus falls clearly short of the normal, basic EU data protection rules and principles.

As will be noted in the analysis of Article 17, below, this defect in the Umbrella Agreement is carried through to the implementation of the "right to rectification".

Ensuring the accuracy of data before sending it, and informing the receiving authority as soon as any inaccuracy becomes apparent, is of course crucial in contexts in which surveillance or repressive action is at stake.

Article 9: Information Security

The Parties shall ensure that they have in place appropriate technical, security and organizational arrangements for the protection of personal information against all of the following:

(a) accidental or unlawful destruction;

(b) accidental loss; and

(c) unauthorized disclosure, alteration, access, or other processing.

Such arrangements shall include appropriate safeguards regarding the authorization required to access personal information.

Analysis: In this respect, there are again some differences with the normal, basic EU rules. First of all, the EC Directive requires protection against "alteration" full stop – not just against "*unauthorized* alteration", although that could perhaps be read into the directive. More importantly, the Directive stipulates that controllers must implement "appropriate technical and organizational measures" to protect against not just the above-mentioned specific kinds of wrongful actions, but against "*all other unlawful forms of processing*" (Art. 17(1)). That is missing from the Umbrella Agreement. It relates to questions of supervision and remedies, as further discussed in the analyses of Articles 18, 19 and 21, below.

Article 10: Notification of an information security incident

1. Upon discovery of an incident involving accidental loss or destruction, or unauthorized access, disclosure, or alteration of personal information, in which there is a significant risk of damage, the receiving Competent Authority shall promptly assess the likelihood and scale of damage to individuals and to the

integrity of the transferring Competent Authority's program, and promptly take appropriate action to mitigate any such damage.

2. Action to mitigate damage shall include notification to the transferring Competent Authority. However, notification may:

(a) include appropriate restrictions as to the further transmission of the notification;

(b) be delayed or omitted when such notification may endanger national security;

(c) be delayed when such notification may endanger public security operations.

3. Action to mitigate damage shall also include notification to the individual, where appropriate given the circumstances of the incident, unless such notification may endanger:

(a) public or national security;

(b) official inquiries, investigations or proceedings;

(c) the prevention, detection, investigation, or prosecution of criminal offenses;

(d) rights and freedoms of others, in particular the protection of victims and witnesses.

4. The Competent Authorities involved in the transfer of the personal information may consult concerning the incident and the response thereto.

Analysis: The only significant difference between the definition of an "incident" in Article 10(1) of the Umbrella Agreement and the definition of "personal data breach" in Article 4(9) of the Draft General Data Protection Regulation, is that the latter also includes "*unlawful destruction*" of data. More importantly, however, under Article 10, remedial action – assessment of possible damage and mitigating action – are only required if [the receiving authority feels that] there is "a significant risk of damage". But how such an authority is supposed to decide that this is, or is not, the case without "assess[ing] the likelihood and scale of damage to individuals and to the integrity of the transferring Competent Authority's program", is a mystery.

As the text stands, receiving authorities can too easily avoid consequences for data breaches ("incidents"), by simply claiming that there was, in the specific case, in their view, no "significant risk of damage". Since, in such cases, the authority would also not even have to inform the transferring authority or the data subjects of the data breach (since paras. (2) and (3) also only apply to "incidents" subject to para. (1)), it would be unlikely that any actual damage would become quickly apparent.[11] The "significant risk" *caveat* therefore seriously undermines the very principle of transparency about data breaches.

[11] It is perhaps not incidental that with regard to the Draft GDPR, while the Commission and Parliament want to apply the duty to notify the data protection authorities to all personal data breaches, the Council wants to limit it in a way highly similar to the one included in the Umbrella Agreement. In the June 2015 Consolidated GDPR Text as agreed within the Council, the notification duty would only apply to data breaches "*which [are] likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of data protected by*

In any case, once again, the notification is to be sent, not to the relevant (i.e., where applicable, special LEA-related) data protection authority – i.e., as concerns data breaches in the USA, to the EU and EU Member States DPAs – but to the transferring authority which, as we have noted before, as an LEA, is more likely to focus on good relations with its counterparts than on the protection of the data of persons under scrunity.

Also highly notable is the fact that the Umbrella Agreement does not in any way specify what kind of information should be included in the "notification" of an "incident" to the transferring authority or the data subjects. This is in stark contrast to the elaborate specifications in the Draft General Data Protection Regulation. Thus, under the GDPR, controllers must provide the relevant (competent) DPA, *inter alia* with:[12]

- information as to the nature of the personal data breach, including the categories and number of data subjects concerned and the categories and number of data records concerned;
- a description of the consequences of the personal data breach; and
- a description of the measures taken by the controller: (i) to mitigate the possible adverse effects of the personal data breach that has occured, and (ii) to address the personal data breach (i.e., to avoid such a breach re-occuring).

Under the GDPR, the controller must also "document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken"; and this information too must be made available to the DPA in question.

Some of these matters might well have to be modified in the context of cross-border LEA data exchanges. However, omitting such requirements altogether from the Umbrella Agreement seriously undermines duties of transparency about data breaches between the cooperating agencies and states. The addition of a paragraph merely allowing "consultations" between the agencies in this respect (para. (4)) adds nothing: it demands nothing and does not create a possibility that without the provision would not have existed anyway.

Also particularly noteworthy is that Article 10 seems to require only "mitigation of damages" – presumably, to any data subjects actually affected. It does not seem to require that the receiving authority also take appropriate steps to avoid a recurrence of the breach.

Even the limited duties to notify the transferring LEA and the data subjects in cases where such a duty applies (i.e., where the receiving authority has been willing to concede that there has been a "significant risk of damage") can be restricted or set aside in broadly-phrased circumstances, under paras. (2) and (3).

Thus, first of all, notification can be subjected to "appropriate restrictions as to the further transmission of the notification". There is no indication of what could be deemed to be, or not to be, "appropriate" restrictions. Without such clarification, this suggests excessive

---

professional secrecy or any other significant economic or social disadvantage". (Council Document 9398/15 of 1 June 2015, revised Article 31). The issue is currently under negotiation in the "Trilogues" between the Commission, Parliament and the Council.

[12] See Article 31(2) in the Commission and Parliament versions of the Regulation (between which there are only minor differences). The Council version adds some qualifications, e.g., referring to "the approximate numbers", but still notably retains the principle that a fairly detailed report should be submitted.

discretion on the part of the LEA notifying a breach. More important still, the reference to "restrictions" on the "further transmission [of the notification of the breach]" seems to allow the LEA where the breach occurred to bar the LEA which is informed of the breach from informing any other bodies of the breach, including other bodies in the latter LEA's country – and including possibly even the DPA charged with overseeing the LEA that is so informed. From an EU perspective, that would be outrageous – but it is precisely the view taken by NSAs in relation to international cooperation information.[13] It should be made completely clear that the "restrictions" on "further transmission" in Article 10 do not include any restrictions on the disclosure of data breaches by an informed LEA to at least the DPA overseeing that LEA. Without such clear clarification – and clarification of what are, and what are not, "appropriate" restrictions – this article is again unacceptable from an EU data protection and fundamental rights perspective.

Furthermore, the Agreement does not require an LEA where a breach has occurred to explain or justify its reliance, in cases in which it invokes them, on any of the sweeping exception clauses in paras. (2) and (3), to the transferring LEA (or to a DPA overseeing the latter LEA). As it stands, the text appears to allow the LEA where the breach occurred almost complete freedom to determine for itself whether notifying the LEA (or LEAs) that sent the data that have been compromised might ("may") "endanger national security", or "endanger public security operations", or (in respect of notification of the data subjects affected by the breach), whether notification might "endanger" "public or national security" (any kind of) "official inquiries, investigations or proceedings", "the prevention, detection, investigation, or prosecution of criminal offenses", or "rights and freedoms of others, in particular the protection of victims and witnesses". Presumably, in the EU, the EU or EU Member States' DPAs (either the general ones or those specifically charged with LEA data protection oversight) can supervise the invoking by any EU or EU Member State LEA of any of these exceptions. In the USA, it would be one (or more?) of the various bodies charged with oversight over aspects of the US LEAs' activities (see the analysis of Article 21, below). But there is nothing in the Agreement that would require the oversight bodies in the EU to inform the oversight bodies in the USA (or *vice versa*) of their findings in this respect. Note in particular that the "Cooperation between oversight authorities" provided for in Article 22 is expressly limited to "effective implementation of the provisions of Articles 16, 17 and 18 [of the Umbrella Agreement]", and thus does not extend to actions taken under Article 10.

This turns the broadly-phrased exception clauses into potentially dangerous loopholes.

---

[13] See the *Issue Paper* of the Council of Europe Commissioner for Human Rights, Democratic and effective oversight of national security services, CommDH-IssuePaper(2015)2, May 2015, prepared by Aidan Wills, available at:
https://wcd.coe.int/ViewDoc.jsp?Ref=CommDH/IssuePaper(2015)2&Language=lanAll
This notes the apparently common practice of national security agencies considering bodies overseeing the activities of such agencies in other countries with which they cooperate to be "third parties"; and denying those oversight bodies access to any data disclosed by them to the NSA that is supposed to be supervised, on the basis that the transferring NSA has "originator control" over the information (see, e.g., p. 64). The Commissioner rightly recommends that:

> [States should] ensure that access to information by oversight bodies is not restricted by or subject to the third party rule or the principle of originator control. This is essential for ensuring that democratic oversight is not subject to an efective veto by foreign bodies that have shared information with security services. Access to information by oversight bodies should extend to all relevant information held by security services including information provided by foreign bodies. (Recommendation 16)

In simple terms: Article 10 in its current form is so full of limitations, qualifications and *caveats* that it totally fails to ensure serious transparency about data breaches compromising personal data (including highly sensitive personal data) on EU persons by US authorities. Whenever the US authorities would feel reluctant to inform EU authorities of data breaches relating to (or including) data sent to the US LEAs by any EU- or EU Member State LEA, they could easily find a reason to avoid doing so – and keep the data breach secret. And even when they did inform the relevant EU- or EU Member States' LEAs, they could prohibit those latter (European) LEAs from passing on the information on the data breach to their data protection oversight bodies.

Article 11: Maintaining Records

1. **The Parties shall have in place effective methods of demonstrating the lawfulness of processing of personal information, which may include the use of logs, as well as other forms of records.**

2. **The Competent Authorities may use such logs or records for maintaining orderly operations of the databases or files concerned, to ensure data integrity and security, and where necessary to follow backup procedures.**

Analysis: "Demonstrating lawfulness" to whom? That is the first question that springs to mind, but which is strangely not spelled out. Oddly enough, the reference in para. (2) to "Competent Authorities" – i.e., the LEAs themselves – might suggest that this "demonstrating of lawfulness" is to the LEAs themselves, whereas it should be, at least, to the "oversight bodies" referred to in Article 21, and indeed not just to the oversight bodies when acting within their own country in relation to their own LEAs, but also in relation to "cooperation between oversight bodies", as envisaged in Article 22. But neither Article 21 nor Article 22 in any way refers to the records mentioned in Article 11.

Nor does Article 11 clearly spell out that the records and logs must be created and maintained in such a way as to always allow for ongoing, and also at least *ex post facto*, review of all the actions of the agencies concerned, at least to the extent that those actions affect any matters subject to the Agreement. As written, the article, and in particular para. (2), suggests that the records and logs are intended more for the benefit of the LEAs than to facilitate close oversight.

At the very least, the Umbrella Agreement should expressly spell out (i) that the records and logs must cover all the matters subject to the Agreement; (ii) that they should be tamper-proof (or at least that any tampering must be discernible); and (iii) that the oversight bodies should have full and complete and unhindered access to the records and logs in question, both in relation to their own national oversight and in relation to joint oversight missions. Without such clear stipulations, the Agreement again fails to ensure real, i.e., verifiable and transparent, compliance with the requirements of data protection laws and principles.

Article 12: Retention Period

1. **The Parties shall provide in their applicable legal frameworks specific retention periods for records containing personal information, the object of which is to ensure that personal information is not retained for longer than is necessary and appropriate. Such retention periods shall take into account the purposes of processing, the nature of the data and the authority processing it, the impact on**

relevant rights and interests of affected persons, and other applicable legal considerations.

2. **Where the United States, on the one hand, and the European Union or a Member State on the other, conclude an agreement on the transfer of personal information other than in relation to specific cases, investigations or prosecutions, such agreement will include a specific and mutually agreed upon provision on retention periods.**

3. **The Parties shall provide procedures for periodic review of the retention period with a view to determining whether changed circumstances require further modification of the applicable period.**

4. **The Parties shall publish or otherwise make publicly available such retention periods.**

Analysis: In relation to data retention, this article distinguishes between personal data disclosed in relation to "specific cases, investigations or prosecutions" – i.e., to presumably targeted data disclosed under MLATs and the like – and data that are disclosed under "[any] agreement on the transfer of personal information *other than in relation to specific cases, investigations or prosecutions*" – i.e., under agreements on the providing and sharing of untargeted data in bulk, such as PNR data disclosed under the EU-PNR Agreement of 2012.

In respect of the former (data disclosed in targeted investigations), the article simply stipulates that each party to the Agreement (i.e., the EU and the USA, and presumably also the EU Member States) must:

> provide in their applicable legal frameworks specific retention periods for records containing personal information, the object of which is to ensure that personal information is not retained for longer than is necessary and appropriate.

This is oddly-phrased. The provision does not say that "the legal framework of the parties must ensure that personal data are not retained for longer than is necessary". Rather, the parties must provide for retention periods that have that "object". Why so circumspect?

The provision also does not relate the "necessity" of the retention to the purpose of the processing – i.e., *in casu*, to the "specific cases, investigations or prosecutions" in relation to which the data were transferred.

Furthermore, the addition of the words "and appropriate" suggest that the retention period is not only to be determined by what is "necessary", but also by this "appropriateness". What does that mean? The reference to "other applicable legal considerations" in Article 12(1) is puzzling in this regard, in particular if linked to the ambiguity of the text on "compatible" uses of the data (see the analysis of Article 6(2), where we concluded that the USA could claim that the disclosure of data obtained by one of its law enforcement agencies from an LEA in an EU Member State, for the purpose of investigating a specific (confirmed or suspected) terrorist offence, by that US LEA, to one of the US national security agencies, for general counter-terrorism purposes, is "compatible" with the original purpose of the transfer). Does it mean that in determining the "necessity" and "appropriateness" of a retention period, consideration could be given to the requirements of other laws in the receiving state – such as FISA in the USA? Or any new US law that might impose retention of the relevant data beyond the time for which they are needed for the specific purpose for

which they were transferred? That would seriously undermine the retention-limitation principle.

There is no such second "appropriateness" test in the main EC Data Protection Directive, which simply stipulates that personal data must be:

> kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. (Article 6(e))

As it stands, the text of Article 12 does not appear to ensure that personal data transferred by European LEAs to their US counterparts in relation to specific cases, investigations or prosecutions are not retained by the US authorities for longer than is necessary for those cases, investigations or prosecutions.

In relation to untargeted, suspicion-less bulk data provided by European LEAs to the US LEAs under separate agreements (such as the EU-US PNR Agreement), Article 12(2) stipulates that any such separate agreement must include "a specific and mutually agreed-upon provision on retention periods". Full analysis will therefore depend on what such other treaties stipulate in this regard.

However, given the serious, fundamental problems with compulsory, suspicion-less collection and retention of bulk data in the EU legal order, and in many EU Member States' legal orders, the stipulation in the Umbrella Agreement is in this respect much too lackadaisical. The CJEU has made clear (and recently reaffirmed in *Schrems*) that the very collection of bulk data without any link to specific offences is highly dubious. To simply ignore that is wrong.

In the light of the CJEU's ruling that the Data Retention Directive was invalid *in toto* and *ab initio*, and now the later *Schrems* judgment, the Agreement ought to specify, first of all, that information on individuals not in any way linked to specific cases, investigations or prosecutions should only be transferred from the EU to LEAs in the USA in exceptional cases provided for in EU instruments that meet the requirements of the Charter and the Treaties, as interpreted by the Court; and that those data should not be retained by the receiving agency for any longer than is strictly necessary to achieve the specific exceptional purpose for which they were transferred, which must be specified in the special instrument; and that the data may not be disclosed by the US LEA in question to any other (US or third country-) body or agency.

As it stands, Article 12 of the Umbrella Agreement does not in any way ensure compliance with the Court's case law.

"Making public" the various data retention periods, and "periodically reviewing" them (paras. (3) and (4)), does not do anything in that regard.

Article 13: <u>Special Categories of Personal Information</u>

1. Processing of personal information revealing racial or ethnic origin, political opinions or religious or other beliefs, trade union membership or personal information concerning health or sexual life shall only take place under appropriate safeguards in accordance with law. Such appropriate safeguards may include: restricting the purposes for which the information may be processed, such as allowing the processing only on a case by case basis; masking, deleting or

blocking the information after effecting the purpose for which it was processed; restricting personnel permitted to access the information; requiring specialized training to personnel who access the information; requiring supervisory approval to access the information; or other protective measures. These safeguards shall duly take into account the nature of the information, particular sensitivities of the information, and the purpose for which the information is processed.

2. **Where the United States, on the one hand, and the European Union or a Member State on the other, conclude an agreement on the transfer of personal information other than in relation to specific cases, investigations or prosecutions, such agreement will further specify the standards and conditions under which such information can be processed, duly taking into account the nature of the information and the purpose for which it is used.**

Analysis: The "special" (i.e., "sensitive") categories of data listed in Article 13(1) are essentially the same as those listed in Article 8(1) of the 1995 Data Protection Directive. However, the Agreement does not take into account that Article 8 of the Directive also places restrictions on the processing of data on "offences, criminal convictions or security measures" (see Article 8(5)). It also, unlike the Directive, does not start from a presumption that the processing of sensitive data should in principle be prohibited, subject to limited, strictly-phrased exceptions (which, as exceptions, must moreover be narrowly interpreted).

What is more, the concept of sensitive data is being significantly developed in the context of the drafting of the General Data Protection Regulation – and this too is not reflected in the Agreement.

Thus, in the course of the process, Parliament has changed "sex life" to "sexual orientation", added "gender identity", "trade union activities", "genetic" and "biometric" data to the main list, and replaced "data concerning ... criminal convictions or related security measures" (the words proposed by the Commission) with "data concerning ... administrative sanctions, judgments, criminal or suspected offences, convictions or related security measures" (see the Commission and Parliament versions of Article 9(1) of the Draft Regulation). The Council stuck mostly with the Commission list, but still also added "genetic data" to the categories deemed sensitive (see Article 9(1) in the consolidated Council version of June 2015). All parties also want to add further important detail on what constitutes "genetic data" and "biometric data" and "data concerning health" (see the Commission, Parliament and Council versions of Article 4, paras. (10), (11) and (12).[14] For example, both the Commission and Parliament consider information which "relates to ... the provision of health services to the individual" as "health data" and thus sensitive. In the USA, such data is generally treated under the "third party" rule as not only not sensitive but essentially freely tradeable.

It is therefore clear that the Agreement does not treat all the data that are already regarded as sensitive in EU data protection law, or that will soon be explicitly so regarded, as sensitive. This is extremely likely to lead to processing by receiving US LEAs of the data contrary to EU law.

[14] "Genetic data" and "biometric data" have also been expressly added to the list of sensitive data in the revised (2014) version of the Council of Europe Data Protection Convention (Convention No. 108).

This view is reinforced by the weak reference in the first sentence of Article 13(1) to "appropriate safeguards in accordance with law". The second and third sentences do little to clarify what is to be meant by that. The second sentence list a number of matters that "*may* [be] include[d]" in such "appropriate safeguards" – but the very wording makes clear that they need not be included. It is informative to re-read the second sentence in that light. It then shows that under the Agreement it may not be necessary in all cases:

- to restrict the purposes for which the sensitive information may be processed to processing on a case by case basis – in other words, in some cases sensitive information may be used in non-targeted activities, typically for data mining and profiling;
- to mask, delete or block the information after effecting the purpose for which it was processed – which non-masking/deleting/blocking would be in breach of the purpose-limitation and data retention principles;
- to restrict [the number of] personnel permitted to access the information;
- to provide specialized training for personnel with access to the sensitive information;
- to require supervisory approval for access to the information; or
- to take other protective measures.

This ambiguity (to put it midly) is yet further compounded by the reference in the first sentence to "in accordance with law". Presumably, this here means the law of the receiving authority. However, as noted, US law as it stands is generally, and also especially in a law enforcement context, much more lax on the processing of sensitive data than EU law. If the "appropriateness" of the adoption of any of the above-mentioned possible safeguards is going to be determined by these lax US laws, then the special protections accorded to sensitive data under EU law is certain to be seriously undermined once such data are transferred to the US LEAs.

The Agreement in this respect also fails to ensure compliance with the, in Europe, seminal instrument on the processing of personal data in the police sector: Council of Europe Committee of Ministers Recommendation No. R(87)15,[15] which is in fact binding on the EU law enforcement bodies.[16] This stipulates in point 2.4 that:

> The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law

[15] Recommendation No. R (87) 15 of the Council of Europe Committee of Ministers, Regulating the Use of Personal Data in the Police Sector, adopted on 17 September 1987. It is worth noting that the UK "reserved the right ... to comply or not" with (*inter alia*) this principle. The Recommendation is currently under review. However, for now, R(87)15 remains the most important set of basic European principles in this area.

[16] R(87)15 is effectively binding on the EU law enforcement agencies, such as Europol, because it is expressly stipulated to contain the data protection standards to which these agencies must conform in various European police co-operation instruments, including the Schengen and Europol treaties and associated regulations; it is also regularly invoked in recommendations by the Parliamentary Assembly of the Council of Europe and its Committee of Ministers, as well as by the European Parliament. See the *Issue Paper* of the Council of Europe Commissioner for Human Rights, Protecting the right to privacy in the fight against terrorism, CommDH/IssuePaper(2008)3, December 2008, prepared by Douwe Korff, available at: https://wcd.coe.int/ViewDoc.jsp?Ref=CommDH/IssuePaper(2008)3&Language=all

> should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry.

The Umbrella Agreement does not contain anything like these restrictions.

On the contrary: Article 13(2) expressly envisages the transfer of "such data" – i.e., of sensitive personal data – under other agreements "other than in relation to specific cases, investigations or prosecutions". Rather than prohibiting such transfers for untargeted data collecting and -mining, as should be done under Recommendation R(87)15, it says that such (other) agreements should "further specify the standards and conditions under which such information can be processed, duly taking into account the nature of the information and the purpose for which it is used." That is direct conflict with the (in the EU: effectively binding) Recommendation.

As further discussed in the analysis of Article 15 on "automated decision-making", below, there is also nothing in the Agreement on the use of sensitive data in profiling generally, or to counter the risk that this may result in direct or indirect discrimination in particular. Given the serious concerns about profiling, this too is an egregious omission.

Article 14: <u>Accountability</u>

1. The Parties shall have in place measures to promote accountability for processing personal information within the scope of this Agreement by their Competent Authorities, and any other of their authorities to which personal information has been transferred. Such measures shall include notification of the safeguards applicable to transfers of personal information under this Agreement, and of the conditions that may have been imposed by the transferring Competent Authority pursuant to Article 6(3). Serious misconduct shall be addressed through appropriate and dissuasive criminal, civil or administrative sanctions.

2. The measures set out in paragraph 1 shall include, as appropriate, discontinuation of transfer of personal information to authorities of constituent territorial entities of the Parties not covered by this Agreement that have not effectively protected personal information, taking into account the purpose of this Agreement, and in particular the purpose and use limitations and onward transfer provisions of this Agreement.

3. In case of allegations of improper implementation of this Article, a Party may request the other Party to provide relevant information, including, where appropriate, regarding the measures taken under this Article.

<u>Analysis</u>: It is unclear how this provision could actually achieve accountability. First of all, although it also refers to accountability for processing by the "Competent Authorities" to which the Agreement is mainly addressed (i.e., the EU-, EU MS- and US LEAs) themselves, it appears to focus on misconduct by others than those "Competent Authorities". Thus, the:

> notification of the safeguards applicable to transfers of personal information under this Agreement, and of the conditions that may have been imposed by the transferring Competent Authority pursuant to Article 6(3) –

can only refer to such "notification" of a third party to which the data are transferred, by the receiving "Competent Authority": that original receiving authority itself of course does not need to be still notified of these safeguards and conditions, as it will have been told of

them when it received the data. It is also clear from the rather obscure reference to the sanction for "not effectively protecting" personal information, consisting of:

> discontinuation of transfer of personal information to authorities of constituent territorial entities of the Parties not covered by this Agreement that have not effectively protected personal information.

The transfer that is here to be "discontinued" can only be a *further* transfer, by the receiving authority, to some other body, here referred to as "authorities of constituent territorial entities of the Parties not covered by this Agreement". Who does this refer to? In our view, these "entities" can only be the parties' – and in particular the US's – national security agencies.

This confirms our suspicion that this whole Agreement is as much about opening further routes through which EU- and EU Member States' LEAs can feed data into the massive US global surveillance programmes, as it is about actual straightforward law enforcement cooperation.

In any case, the "measures to promote accountability" are almost risibly feeble. There is no specific protection for whistle-blowers, who are in practice a key means of ensuring accountability. Otherwise, apart from the above-mentioned duty to notify the third-party recipient of the data of any relevant "safeguards" and "conditions" imposed by the transferring authority, they consist of:

- the imposition of "appropriate and dissuasive criminal, civil or administrative sanctions" for "serious misconduct" – which surely are always already in place in any rule-of-law state? And is there no need for sanctions against lesser "misconduct"? How are "serious" and "lesser" misconduct defined?
- "discontinuation" of the passing on of data to the third-party agency (presumably, an NSA, including the US NSA, or at least including such agencies), if the third party agency did "not effectively protect[] [the] personal information [disclosed to it]", i.e., if the third-party agency actually suffers a data breach.

Notably, the article does <u>not</u> say that there should always be effective sanctions against any processing of the data received by the third party contrary to the "safeguards" and "conditions" originally stipulated by the transferring agency. In particular, "misconduct" must presumably be read as conduct contrary to the rules of the agency in question. Unless this were to be spelled out, it cannot be assume that not adhering, by the third-party agency, to the "safeguards" and "conditions" imposed by the original transferring authority always automatically, *ipso facto*, constitutes "misconduct" on the part of the third-party agency, or any staff member of the agency, in question. Moreover, there is nothing in the article to suggest that if the third-party agency processes the data in breach of these "safeguards" and "conditions", but without actually loosing them ("not effectively protecting" them), any sanctions need to be imposed, let alone the passing on "discontinued".

The final paragraph, which says that:

> In case of allegations of improper implementation of this Article, a Party may request the other Party to provide relevant information, including, where appropriate, regarding the measures taken under this Article –

is useless in terms of ensuring "accountability", even between the parties. All that a party (the EU, an EU Member State, or the USA) may do is "*request* the other Party to provide relevant information"; and that may include, "where appropriate" (!), information "regarding the measures taken" in response to any "improper implementation of this Article". There is no requirement that the other party must actually provide the information. Moreover, the transferring party can, under this article, only ask for information in relation to "allegations of improper implementation of this Article" – not, it would seem, about allegations of non-compliance with the "safeguards" and "conditions" it stipulated, or more generally about allegations of non-compliance by the other party with any other requirements of the Umbrella Agreement.

In simple terms: Article 14 does not in any way ensure accountability of the parties in respect of their compliance, or non-compliance, with the Agreement. There is not even proper accountability between the parties, and certainly no accountability towards the general public, oversight bodies (see also the analysis of Article 21, below), parliaments or the general public.

Article 15: Automated Decisions

Decisions producing significant adverse actions concerning the relevant interests of the individual may not be based solely on the automated processing of personal information without human involvement, unless authorized under domestic law, and with appropriate safeguards that include the possibility to obtain human intervention.

Analysis: The use of data mining, profiles and algorithms to underpin decision-making is one of the most worrying trends in recent years, accelerated by the ever-increasing amounts of personal data (and of non-personal-, e.g., statistical data that are however still applied to individuals). The algorithms, especially if "dynamic" or "self-learning", quickly become incomprehensible even to those relying on them; their outcomes tend to reinforce social biases and lead to discrimination; and decisions taken on the basis of such algorithms become effectively unchallengeable. This is the case *a fortiori* if the data mining and profiling is done in a law enforcement- or anti-terrorist/national security context, especially if the aim is to "identify" people who *may* be terrorists or serious criminals.

(This is different from the limited use of information technology to, for instance, compare details of the *modus operandus* of a criminal with recorded details from another crime scene. That does not involve full-automated, "dynamic", "self-learning" and predictive algorithms, but only the straightforward processing and comparing of factual data.)

As it was put in a recent report for the Council of Europe:[17]

> "[P]reventive" or "predictive" profiling of individuals on the basis of essentially unverifiable and unchallengeable "dynamic"-algorithm-based mining of bulk data, unrelated to any specific indications of wrongdoing, and without any targeting on the basis of such suspicions does touch on the "essence", the untouchable core of the right to privacy – and indeed violates the even more fundamental principle underpinning the right to privacy (and other rights), that states must respect "human identity".

[17] Douwe Korff & Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards (footnote 3, above), section I.iii, *The dangers inherent in data mining and profiling*, pp. 22-37. See there for a detailed discussion of the issues relating to such activity.

The authors concluded that the various EU-third country instruments allowing for such datamining and profiling without adequate safeguards, including the new EU-US PNR Agreement – which is one of the instruments covered by the Umbrella Agreement – were therefore "incompatible with European legal principles of the most fundamental kind."[18]

The question then is whether the above provision in the Umbrella Agreement does anything to prevent such dangerous profiling – profiling which is also unlawful from a human rights perspective, since the methods used are not predictable enough to be considered "prescribed by law" under European jurisprudence. The answer is No.

Thus, first of all, the article expressly allows quite generally for the taking of decisions on the basis of "automated processing of personal information" – i.e., read here: data mining and profiling – as long as there is some form of "human involvement". This ignores what is known as "automation bias", a well-documented phenomenon, caused by "the propensity for humans to assume that automated decision making systems are infallible and to ignore contradictory information made without automation, even if it is correct."[19] In a law enforcement/anti-terrorist context, it is also extremely unlikely that the "human involvement" will include any opportunity on the part of the person affected by the decision (e.g., a person who is labelled "high risk" on an anti-terrorist database) to argue against the decision, or the ranking, or to put forward facts or arguments against them. Indeed, as noted in the analysis of Article 16, below, unlike under the EU instruments, under the Umbrella Agreement data subjects are not even entitled to basic information on the "logic" used in automated decisions that affect them.

The effectiveness of the "human involvement" requirement of Article 15 must therefore be regarded as inherently largely meaningless.

But beyond that, automated decisions based on profiles and algorithms are actually also allowed *without any "human involvement"* under Article 14 of the Agreement, provided only that this is "authorized under domestic law" (i.e., the law of the receiving authority), and provided that "appropriate safeguards" are in place (although it is not stipulated that those safeguards need to be spelled out in the relevant law itself). These "appropriate safeguards", the article goes on to say, must "*include the possibility* to obtain human intervention". In other words, as long as there is, under the relevant domestic law, a "possibility" for a human to intervene, the automated decision can be allowed to stand; there need not have been any *actual* human intervention.

This stands in direct contrast to the view of the European Parliament, that:

> Profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject shall not be based solely or predominantly on automated processing and **shall include human assessment**, including an explanation of the decision reached after such an assessment.
>
> (Article 20(5) of the EP version of the GDPR, emphasis added)

---

[18] *Idem*, p. 94, emphasis omitted.

[19] See Rachel O'Connor, Is Cameron proposing to legislate, inadvertently, for a Police State in the UK? Why citizens should urge caution, balance and proportionality, 21 January 2015, on the "TrustElevate" *groovyfuture* blog, available here: http://groovyfuture.com/is-cameron-proposing-to-legislate-inadvertently-for-a-police-state-in-the-uk-why-citizens-should-urge-caution-balance-and-proportionality/

It would be odd indeed if the EU, following the Parliament proposal, were to prohibit the taking of significant decisions on the basis of profiles without human intervention in the EU, but would (by ratifying the Umbrella Agreement) allow US LEAs – and indeed the NSA – to take such decisions without human intervention, in respect also of people living in the EU (be they EU citizens or asylum seekers or refugees) or travelling to, from or through the EU.

Moreover, as already noted in the analysis of Article 13, above, there is also nothing in the Agreement – and here we can add: in Article 15 in particular – on the use of sensitive data in profiling generally, or to counter the risk that this may result in discrimination in particular. This is in stark contrast to the rules on profiling in the Draft General Data Protection Regulation. In that respect, the Commission and Parliament agree that:

> **[Profiling] shall not be based solely on [sensitive data].**
>
> (Article 20(3) of both the Commission and the Parliament versions of the GDPR)

In fact, Parliament wants to add the following to this:

> Profiling that has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity, or that results in measures which have such effect, shall be prohibited. The controller shall implement effective protection against possible discrimination resulting from profiling.
>
> (Added text to Article 20(3) in the EP version)

This would be a very important, positive addition to the Regulation, given the very real risks of discrimination becoming (even inadvertently) entrenched in algorithm-based decision-making.[20]

The absence from the Umbrella Agreement of stipulations on the lines of those proposed for the Regulation by the European Parliament are, as we already said, egregious omissions.

Given the very serious repercussions that decisions or determinations by law enforcement and anti-terrorist agencies can have for the individuals concerned – especially if those can be shared with yet other agencies in yet other countries – Article 15 provides for an unacceptably lax regime for automated decision-making by such agencies.

Article 16: Access

1. The Parties shall ensure that any individual is entitled to seek access to his or her personal information and, subject to the restrictions set forth in paragraph 2, to obtain it. Such access shall be sought and obtained from a Competent Authority in accordance with the applicable legal framework of the State in which relief is sought.

2. The obtaining of such information in a particular case may be subject to reasonable restrictions provided under domestic law, taking into account legitimate interests of the individual concerned, so as to:

(a) protect the rights and freedoms of others, including their privacy;

---

[20] See Douwe Korff & Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards (footnote 3, above), sub-section on *Discrimination by computer*, pp. 26 – 28 (with further references).

(b) safeguard public and national security;

(c) protect law enforcement sensitive information;

(d) avoid obstructing official or legal inquiries, investigations or proceedings;

(e) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offenses or the execution of criminal penalties;

(f) otherwise protect interests provided for in legislation regarding freedom of information and public access to documents.

3. Excessive expenses shall not be imposed on the individual as a condition to access his or her personal information.

4. An individual is entitled to authorize, where permitted under applicable domestic law, an oversight authority or other representative to request access on his or her behalf.

5. If access is denied or restricted, the requested Competent Authority will, without undue delay, provide to the individual, or to his or her duly authorized representative as set forth in paragraph 4, the reasons for the denial or restriction of access.

Analysis: Recognition-in-principle of the right of access (and of the right to rectification, under Article 17, analysed separately below) is important: these rights are cornerstones in the European data protection frameworks. However, the proof must be in the application, i.e., in the scope of the right; in whether, and to what extent, these rights can be really effectively exercised in practice; and in whether, and if so when, they can be restricted or denied.

On the first point, it is crucial to note that under the Umbrella Agreement data subjects are not entitled to any (even basic/outline) information on the "logic" used in automated decisions of the kind covered by Article 15, discussed above – i.e., of the kind of logic or algorithms used in data mining and profiling by LEAs (and NSAs), in particular in relation to terrorism. In the context of EU-US law enforcement data exchanges, including transfers of PNR data from the EU or the EU Member States to the USA, which have been shown to be specifically aimed at such data mining and profiling,[21] this is a most serious, glaring omission.

The next point to note is the stipulation in Article 16(1) that:

> Such access shall be sought and obtained from a Competent Authority in accordance with the applicable legal framework of the State in which relief is sought.

In other words, EU citizens must seek access to any data held by US LEAs in accordance with the US legal framework for such access, and subject to the restrictions enumerated in paragraph (2) *as provided for in the US legal framework*.

[21] See Douwe Korff and Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards (footnote 3, above), section I.ii, *The use of airline passenger data for anti-terrorist screening in the USA: CAPPS I & II and "Secure Flight" – and their links to "Total Information Awareness" and now to the NSA/GCHQ global surveillance programmes*, under the sub-heading "recent developments", p. 13ff, in particular the discussion of the "fourth [TSA] list", discussed on pp. 16 – 17.

Here, once again, an immediate contrast with the European standards becomes clear. In Europe, restrictions on fundamental rights must be based on "law" – i.e., on published legal rules that are "clear and precise and foreseeable in their application"; they must serve a "legitimate aim" or "interest"; and they must be "necessary" and "proportionate" in relation to the relevant aim or interest.[22] Those are fundamental, constitutional principles, firmly upheld by the European Court of Human Rights and the CJEU under the ECHR and the Charter, also in relation to the processing of personal data. Since "subject access" is, as just mentioned, a cornerstone of European data protection law, restrictions on that right must, in the EU (and the Council of Europe Member States) also meet these standard tests.

This is reflected in Article 13(1) of the main Data Protection Directive, which stipulates that many of the requirements of the directive, including the duty to allow data subjects access to their data, may be restricted by means of "legislative measures" (read: under legal rules meeting the "quality of law" tests developed by the European courts):

> ... when such a restriction constitutes a necessary measures to safeguard:
>
> (a) national security;
>
> (b) defence;
>
> (c) public security;
>
> (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
>
> (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
>
> (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
>
> (g) the protection of the data subject or of the rights and freedoms of others.

While the interests for which the right of access may be limited are largely similar (except for the last one listed in the Umbrella Agreement, discussed separately, below), the tests applied to any restrictions under the Agreement are much less strict than the fundamental (ECHR/Charter/constitutionally-based) European ones. Thus, first of all, the Agreement says nothing about the "quality" of any US law restricting subject access, thereby allowing for restrictions on access in the USA on the basis of vaguely-worded provisions in US laws that are not "foreseeable" in their application. The text of the Agreement would in fact not even appear to prohibit restrictions on access, based on secret laws or secret interpretations of the US laws (such as have bedevilled the legal regime relating to NSA surveillance).

Secondly, where European human rights- and data protection law requires that any restrictions on subject access must be "necessary" and "proportionate" to the legitimate aim pursued by the restriction, the Agreement allows for restrictions as long as they are "reasonable ... taking into account [the?] legitimate interests of the individual concerned". As any lawyer – and in particular any common law lawyer – knows, a "reasonableness" test

---

[22] See Douwe Korff, The Standard Approach under Articles 8 – 11 ECHR and Article 2 ECHR, at: http://ec.europa.eu/justice/news/events/conference_dp_2009/presentations_speeches/KORFF_Douwe_a.pdf For a summary of the application of these tests in relation to law enforcement and national security, see the Council of Europe *Issue Paper* on The rule of law on the Internet and in the wider digital world (footnote 2, above), section 3.2, *The basic "rule of law" tests developed by the European Court of Human Rights*.

can fall far short of a "necessity" test.[23] The right of access to data under Article 16 of the Agreement may thus be subjected by the US authorities to wider, "reasonable" exceptions than only to the "necessary" and "proportionate" ones that are allowed under European (ECHR and EU) law. There is also no specific requirement to provide access to the data once the ground for refusing access is no longer relevant.

In addition, there is the (again, somewhat oddly-phrased) reference to a legitimate ground for restricting access, contained in paragraph (f). Under this paragraph, data subjects may be restricted or denied access to their data, held by US LEAs, if this is "reasonable ... so as to:"

> ... protect interests provided for in legislation regarding freedom of information and public access to documents.

This is a somewhat strange link to freedom of information (FOI) law. It suggests that any "*interest*" that is protected by US FOI law, and that can be invoked under the Freedom of Information Act (FOIA) in particular, can also be relied upon to restrict or deny access to data held by any US LEA. But notably, as discussed below, it does not say that the *standards* for refusal of FOI requests under the FOIA (i.e., the *tests* stipulates in the FOIA) are also applicable. The exemptions in the FOIA are as follows:[24]

> [The right of access to documents under the US FOIA] does not apply to matters that are--
>
> (1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;
>
> (2) related solely to the internal personnel rules and practices of an agency;
>
> (3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
>
> (4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
>
> (5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
>
> (6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

---

[23] This applies in particular to the "*Wednesbury* unreasonableness" test in English law, which essentially allows actions by public authorities to stand as long as they are not demonstrably and manifestly unreasonable. See Lord Carnwath's speech From Rationality to Proportionality in the Modern Law, given at the joint UCL-HKU conference *'Judicial review in a changing society'*, at Hong Kong University, 14 April 2014, available at:
https://www.supremecourt.uk/docs/speech-140414.pdf
Lord Carnwarth argues that "[t]he actual decision in Wednesbury would be difficult to justify under the modern law, and its days as an authority may be numbered." – precisely because the English courts these days often apply the more demanding "necesssity" and "proportionality" tests of European (EU and ECHR) law.

[24] For brief additional information on the application of each exemption, see:
http://www.foiadvocates.com/exemptions.html

(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information—

(A) could reasonably be expected to interfere with enforcement proceedings,

(B) would deprive a person of a right to a fair trial or an impartial adjudication,

(C) could reasonably be expected to constitute an unwarranted invasion of personal privacy,

(D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source,

(E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or

(F) could reasonably be expected to endanger the life or physical safety of any individual;

(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(9) geological and geophysical information and data, including maps, concerning wells.

(FOIA 5 USC. § 552(b)(1)-(9))

Some of these, such as exemptions (2), (4), (8) and (9), are unlikely to be relevant to subject access requests made to US LEAs by EU citizens or residents or other non-EU citizens whose data may have been transferred to the USA. Others, such as exemptions (6) and (7)(C), which are aimed at protecting the privacy of the data subject, would also appear to be inapplicable in relation to a request by a person for access to her or his own data (although it could mean that information on other persons, included in the file on the person making the access request, may have to be deleted or redacted). The effect of other FOIA exemptions on the application of the Umbrella Agreement is difficult to assess without further information – e.g., on whether there are US Presidential Determinations of secrecy that could cover some relevant information (exemption (1)); on whether there are any other US laws that "specifically exempt" certain LEA data from access (other than as provided for in exemption (7))(exemption (3)); or on whether exemption (5) could be relied upon to limit access more than would be allowed under the European "necessity" and "proportionality" tests.

The exemptions that would seem to be most directly relevant are those contained in exemption (7)(A), (B), (D), (E) and (F). In terms of the interests listed, they are again broadly in line with European standards – which are, if anything, more broadly phrased (see the quote, below).

In terms of the FOIA itself, the relevant tests as to when these interests can be invoked are phrased in different terms than in European law. Thus, the core Council of Europe Recommendation R(87)15, already mentioned, stipulates that:

> Exercise of the rights of access, rectification and erasure should only be restricted insofar as a restriction is **indispensable** for the performance of a legal task of the police or is **necessary** for the protection of the data subject or the rights and freedoms of others.
>
> (Principle 6.4, emphasis added).

If the FOIA tests were to be applied under the Umbrella Agreement, the question would then be whether denial of access on the bases provided for in the FOIA – i.e., that access "*could reasonably be expected to interfere with enforcement proceedings*"; "*would deprive a person of a right to a fair trial*"; "*could reasonably be expected to disclose the identity of a confidential source*"; or "*would disclose techniques and procedures for law enforcement investigations or prosecutions*" – could, in European-legal terms, be said to be "indispensable" for the performance of the legal task of the relevant LEA, or "necessary" for the protection of the data subject or the rights and freedoms of others.

In principle, we feel that in the abstract the answer to that question could therefore be Yes.

However, Article 16(2)(f) of the Umbrella Agreement does <u>not</u> say that the FOIA *tests* apply to data subject requests made by EU persons to US LEAs: it says that access may be subject to "reasonable restrictions" imposed "so as to protect" any of the "*interests*" protected by US FOI law (including the FOIA).

The differences between the tests therefore remain: in the USA, subject access can be denied when this is "reasonable" to protect law enforcement activities, while in Europe, the denial must be "indispensable" to that end.

There is a further matter of importance. Article 16(4) stipulates that individuals can authorise an "oversight body" – in the EU, a Data Protection Authority (DPA) – to request access on her or his behalf. This is also provided for in many European systems with regard to access to LEA data. However, in the EU, in such cases, the DPA is granted full access to the LEA data (except perhaps while active investigations are still continuing) and can order correction or erasure – even if the data subject will often not be informed in detail of the action taken. But under the Umbrella Agreement, such a designated DPA is *not* entitled to full access to the data. Under the Umbrella Agreement, a thus-designated European DPA would, as far as subject access is concerned, be essentially in the same position as anyone else who might be authorised by the data subject to act on the latter's behalf (e.g., a European-, or indeed a US NGO): the DPA (or the NGO) does not have any right of further access than the data subject her- or himself. If a European data subject is denied access to data held by a US LEA, or granted only limited access, any European DPA acting on the data subject's behalf would be subject to those very same restrictions.

Moreover, as noted in the analyses of Articles 18 and 21, below, the relevant "oversight bodies" in the USA are also not granted the kind of full access given to LEA data in the above-mentioned EU systems.

Enforcement of subject access is therefore, under the Agreement, also much weaker in the USA than in the EU.

Article 17: Rectification

1. The Parties shall ensure that any individual is entitled to seek correction or rectification of his or her personal information that he or she asserts is either inaccurate or has been improperly processed. Correction or rectification may include supplementation, erasure, blocking or other measures or methods for addressing inaccuracies or improper processing. Such correction or rectification shall be sought and obtained from a Competent Authority in accordance with the applicable legal framework of the State in which relief is sought.

2. Where the receiving Competent Authority concludes following:

(a) a request under paragraph 1;

(b) notification by the provider; or

(c) its own investigations or inquiries;

that information it has received under this Agreement is inaccurate or has been improperly processed, it shall take measures of supplementation, erasure, blocking or other methods of correction or rectification, as appropriate.

3. An individual is entitled to authorize, where permitted under applicable domestic law, an oversight authority or other representative to seek correction or rectification on his or her behalf.

4. If correction or rectification is denied or restricted, the requested Competent Authority will, without undue delay, provide to the individual, or to his or to her duly authorized representative as set forth in paragraph 3, a response setting forth the basis for the denial or restriction of correction or rectification.

Analysis: Much of what has been said above in relation to subject access (Article 16) also applies to the right to correction or rectification. Thus, the latter right is also to be granted in the way, and to the extent, that this is *provided for in the US legal framework*, which, as we have noted, in particular does not require that the right is laid down in clear and precise, published law that is foreseeable in its application. Furthermore, although a European data subject can again authorise the relevant (possibly LEA-specific) DPA of her or his own Member State – or, in respect of data sent to the USA by a EU law enforcement institution, the EDPS – to act on her or his behalf (Article 17(3)), the latter can again not act as a DPA would be able to do in many EU Member States, and get full access to the data (while being restricted in what can be disclosed to the data subject). Rather, the European DPA would not be allowed to check for itself whether, in its view, the data need "correcting" or "rectifying" (as further discussed below). Rather, the determination of whether any data that are being challenged as being inaccurate or as having been "improperly processed" is again left to the US LEA in question.

Moreover, again, as noted in the analyses of Articles 18 and 21, below, the relevant "oversight bodies" in the USA are also not granted the kind of full access given to LEA data in the above-mentioned EU systems.

Like enforcement of subject access, enforcement of the right to rectification is therefore, under the Agreement, also much weaker in the USA than in the EU.

There is a further major issue, which concerns the question of what remedial action is "appropriate" in relation to what kinds of errors in the data. The analysis of Article 8, above, already noted that that article fails to spell this out. Here, we note that Article 17 is also unclear about this, in spite of the stipulation in its first paragraph that:

> Correction or rectification may include supplementation, erasure, blocking *or other measures or methods for addressing inaccuracies or improper processing* –

and the similar stipulation in the second paragraph that "where the receiving Competent Authority concludes [of its own motion, or in response to a data subject access and/or rectification request, or because of information provided by the transferring authority] that information it has received under this Agreement is inaccurate or has been improperly processed":

> it shall take measures of supplementation, erasure, blocking or other *methods of correction or rectification*, as appropriate.

The ambiguity lies in the reference to "other measures or means for addressing inaccuracies or improper processing". In Europe, it is made increasingly clear in the relevant instruments in particular that if it has been shown that personal data have been or are "improperly processed", they should be **erased**.

This was already suggested in the 1995 Data Protection Directive: see Article 5(d), quoted in the analysis of Article 8, above, and Article 12. It is made more explicit in the shortly-to-be-adopted General Data Protection Regulation. In Article 16 and 17, this distinguishes between "rectification" of "inaccurate" data, "completion" of "incomplete" data, and "erasure" of data that has been, or is being, processed contrary to the provisions of the Regulation, as follows:

> Article 16
>
> **Right to rectification**
>
> The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement.
>
> Article 17
>
> **Right to be forgotten and to erasure**
>
> 1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:
>
> (a) ...
>
> (b) ...
>
> (c) ...
>
> (d) the processing of the data does not comply with this Regulation for [any] other reasons.

Exceptions to this duty to erase improperly processed data are limited in accordance with the standard principles of European human rights- and data protection law: such exceptions

must be "necessary" for compliance with a "legal obligation" (i.e., an obligation laid down in a law that must meet the "quality" requirements of law, developed by the European courts); and that legal obligation (i.e., that law) must itself "meet an objective of public interest", "respect the essence of the right to the protection of personal data" and be "proportionate" in relation to the legitimate aim pursued (Article 17(3) of the GDPR).

As already noted in the analysis of Article 8, above, the omission of any reference to a duty on the part of any "competent authority" to "delete" or "erase" data that are processed contrary to the Umbrella Agreement is the more worrying in the light of the binding Explanatory Note on the EU-US MLAT, already quoted in the analysis of Article 1(3), above, according to which:

> [The fact that] the requesting State [NB: that would under the Umbrella Agreement be the state receiving the data] uses **means other than the process of deletion to protect the privacy or the accuracy of the personal data** received by law enforcement authorities [may not be invoked by the transferring state as a reason for not transferring the data, or to impose "generic conditions" on the transfer, e.g., that erroneous data be erased].

Clearly, the US authorities are determined to avoid any formal legal requirements, under the Umbrella Agreement or under EU-US MLAT of 2003, to ever fully delete data, even if the data were shown to be inaccurate and/or processed in violation of the Agreement (or the MLAT); let alone to any formal requirement to inform third parties to whom the inaccurate or improperly processed data were transferred, of such a need for deletion.

Once again, therefore, the Umbrella Agreement (and for that matter, the EU-US MLAT of 2003) thus falls clearly short of the normal, basic EU data protection rules and principles – here: in respect of the right to correction *or deletion* of inaccurate or improperly processed data.

This is not in any way remedied by the stipulation in the final paragraph of Article 17 that:

> If correction or rectification is denied or restricted, the requested Competent Authority will, without undue delay, provide to the individual, or to his or to her duly authorized representative as set forth in paragraph 3, a response setting forth the basis for the denial or restriction of correction or rectification.

This stipulation suffers from two defects. First of all, since in the view of the US authorities "means other than deletion" can suffice "to protect the privacy or the accuracy of the personal data", even in respect of data that are inaccurate or that have been – or still are! – "improperly processed", the US receiving authority will presumably not regard the use of such "other means" as a "denial or restriction" of the right to correction or rectification. In that case, they would not even "provide a response" to the EU person (or to any EU DPA representing him or her), explaining the "other means" used. And unlike in the EU, the EU DPA representing the EU data subject would also not be given any insight into those "other means" either, or even be informed of the action taken (or not taken).

Even when the US authorities accept that their response to a request for rectification amounts to a "denial or restriction" of that right, Article 17(4) does not require that those authorities provide the *reasons* for that denial or restriction. Rather, they only have to inform the data subject – and/or the EU Member State DPA involved – of the *basis* for the denial or restriction. That "basis" could simply be said to be the relevant US law. Furthermore, the relevant provisions on appeals are weak (see the discussion of Article 18,

below). They do not amount to an effective right of appeal against a refusal to correct or delete contested data, such as is typically provided for in the laws of the EU Member States.

This means that the scope of any action or inaction by US authorities responding to access and rectification requests from EU data subjects can be obscured and left effectively unexplained by the US authorities, without the EU DPAs having any real insight or input in this either. And with the US "oversight bodies" also not granted the kind of full access given to LEA data in the above-mentioned EU systems (as further discussed in the analyses of Articles 18 and 21, below).

In sum: in respect of the right to rectification too, the Umbrella Agreement fails to meet the European basic standards, both in terms of scope and substance, and in terms of enforcement powers and –arrangements.

Article 18: Administrative Redress

1. **The Parties shall ensure that any individual is entitled to seek administrative redress where he or she believes that his or her request for access pursuant to Article 16 or rectification of inaccurate information or improper processing pursuant to Article 17 has been improperly denied. Such redress shall be sought and obtained from a Competent Authority in accordance with the applicable legal framework of the State in which relief is sought.**
2. **An individual is entitled to authorize, where permitted under applicable domestic law, an oversight authority or other representative to seek administrative redress on his or her behalf.**
3. **The Competent Authority from which relief is sought shall carry out the appropriate inquiries and verifications and without undue delay shall respond in written form, including through electronic means, with the result, including the ameliorative or corrective action taken where applicable. Notice of the procedure for seeking any further administrative redress shall be as provided for in Article 20.**

Analysis: There are three main issues that arise under this article. First of all, it would seem to be a great step forward that for once, here we seem to have a provision that extends a right – *in casu*, the right to "administrative redress" – to "any individual": Article 18 stands out as not being limited to "citizens" or "nationals" of the parties, i.e., of the EU Member States and the USA. However, given that we find below that the redress offered by this article is in fact of little real value, and especially in view of the limitation of the right to judicial redress under Article 19 to "citizens" of the EU and the USA, inequality and discrimination are retained in this crucial respect – as further discussed in the analysis of Article 19.

Secondly, the redress provided for in Article 18 is limited to (alleged) denials of requests by data subjects for access to their data under Article 16 and/or "rectification of inaccurate information or improper processing" under Article 17. Moreover, crucially, such complaints are to be handled "in accordance with the applicable legal framework of the State in which relief is sought", i.e., in respect of complaints brought by EU data subjects relating to processing of data on them by US receiving authorities, in accordance with the US legal framework. To the extent that this US legal framework, in scope or substance, falls short of European basic principles – as our analyses show it repeatedly does – Article 18 therefore does not provide any remedy.

For instance, a European data subject cannot obtain, from the US authorities, the deletion of data on him or her that have been processed in violation of the Umbrella Agreement (or of any other agreement to which the Umbrella Agreement applies, such as the EU-US MLAT), if that is not provided for in US law – even though such a data subject could demand such deletion of any EU LEA, if the data were processed by the latter.

Secondly, it should be noted that the "administrative redress" provided for in Article 18 is an **entirely internal, self-policing** one: the authority to which a European data subject should address a request for redress is the very same US receiving authority about which the complaint is made. All that the "redress" amounts to is therefore a "right" (if it can be called that) of the data subject to meekly ask the authority about which he or she complains to review the processing of the data, and the handling of the initial request for access and/or rectification.

Once again, the possibility provided for in the second paragraph, for the data subject to authorise an EU Member State DPA (or the EDPS) as a "representative" in this respect adds little: the data subject and the European DPA will be informed in writing of the "result" of the review, "including the ameliorative or corrective action taken where applicable" (Article 18(3)), but if the data subject does involve a European DPA, that DPA is given no more standing or right of input than the data subject him- or herself. The European DPA would not be involved in the actual review. And the same applies if the data subject appoints an NGO as his or her representative.

It is therefore difficult to see how the "administrative redress" provided for in Article 18 can be of any real value.

This makes the question of "judicial redress" – much highlighted as a major, perhaps indeed the main, achievement of the Umbrella Agreement – even more important. It is analysed next.

Article 19: Judicial Redress

1. The Parties shall provide in their applicable legal frameworks that, subject to any requirements that administrative redress first be exhausted, any citizen of a Party is entitled to seek judicial review with regard to:

(a) denial by a Competent Authority of access to records containing his or her personal information;

(b) denial by a Competent Authority of amendment of records containing his or her personal information; and

(c) unlawful disclosure of such information that has been willfully or intentionally made, which shall include the possibility of compensatory damages.

2. Such judicial review shall be sought and obtained in accordance with the applicable legal framework of the State in which relief is sought.

3. Paragraphs 1 and 2 are without prejudice to any other judicial review available with respect to tlie processing of an individual's personal information under the law of the State in which relief is requested.

4. In the event of the suspension or termination of the Agreement, articles 26(2) or 29(3) shall not create a basis for judicial redress that is no longer available under the law of the Party concerned.

Analysis: This article, and the Judicial Redress Bill to which it refers (without expressly naming it) has been hailed as the greatest achievement of the Umbrella Agreement. It therefore deserves particularly close attention and analysis. Unfortunately, once again, such an analysis shows that it does not live up to what it seems to promise.

First of all, unlike the (largely meaningless) "administrative redress" offered by Article 18 to "any individual", irrespective of nationality or citizenship, the "judicial redress" offered by Article 19 is expressly limited to "any citizen of a Party" – i.e., to EU and US "citizens".

Thus, **non-EU people** living in EU Member States who are not nationals of the Member State concerned – such as Syrian refugees or Afghan or Eritrean asylum-seekers, or students from Africa or South America or China – and **non-EU citizens** who have flown to, from or through the EU and whose data may have been sent to the USA (in particular, under the EU-US PNR Agreement), are all **completely denied judicial redress in the USA under the Umbrella Agreement**.

In fact, ironically, until and unless Denmark, the UK and Ireland join the Umbrella Agreement, their own citizens are also completely denied such judicial redress in the USA because the Agreement – and thus also Article 19 – does not cover them until that happens (Article 27).

This stands in direct contrast to the fundamental position laid down in the EU Charter of Fundamental Rights, reflecting the core principle of universality of human rights in all the main international and European human rights treaties. This first of all stipulates, in Article 47(1), as follows:

> Article 47
>
> **Right to an effective remedy and to a fair trial**
>
> **Everyone** whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.

The main condition is the one set out in the next paragraph, which spells out the

> Everyone is entitled to **a fair and public hearing** within a reasonable time by an **independent and impartial tribunal previously established by law**. Everyone shall have the possibility of being advised, defended and represented.

The words highlighted in bold emphasize two aspects of the right:

- it must be accorded to "**everyone**" whose rights and freedoms, as enshrined in the Charter, are affected; and
- the remedy must essentially be a **judicial remedy**: the "tribunal" referred to may be a specialised one, but it must bear all the hallmarks of a judicial body, in particular in terms of independence and impartiality, and of fairness and procedural correctness.

Since the Charter guarantees data protection to everyone whose data are processed under EU law (Article 8), the EU and the Member States must also guarantee the "procedural aspect" of that right, as enshrined (for it and all Charter rights) in Article 47.

In our view, the failure to provide, in the Umbrella Agreement, for judicial redress for non-EU persons whose data are disclosed to the USA subject to the Agreement and then proven to be inaccurate, or processed in breach of the Agreement, is in breach of Article 47, read together with Article 21 of the Charter.[25]

Even when the judicial redress provided for in Article 19 does apply, it is expressly limited, both in terms of scope and in terms of available kinds of redress offered to EU citizens. In terms of scope, it is limited to the following:

> (a) denial by a Competent [for EU citizens, read: US] Authority of access to records containing his or her personal information;
>
> (b) denial by a Competent [US] Authority of amendment of records containing his or her personal information; and
>
> (c) unlawful disclosure of such information ...

Of course, since these matters are again to be determined in accordance with the "legal framework" of the receiving authority and the judicial review body (Article 19(2)) – i.e., for EU citizens, the US legal framework – any determination of such claims will be made in accordance with the rules on denial of access and "amendment" of records (read: "rectification" and "correction" of the information), and in accordance with any exceptions or qualifications of those rules, provided for in US law. In the analyses of Articles 16 and 17, we have shown that in these respects, US law falls short of basic EU data protection requirements. In particular, these showed that US law does not appear to require deletion or erasure of inaccurate data, or even of data that have been "improperly processed", more specifically, that have been processed in breach of the Umbrella Agreement itself, in circumstances in which such deletion or erasure would be required under EU data protection law. Article 19 by its very nature, as a domestic US judicial remedy operating within the US legal framework, does nothing to remedy that defect. The most the relevant US judicial body could do would be to order the relevant (receiving) US authority to take such remedial action as might be provided for within that framework, i.e., to grant access, or to append a "corrective statement" to the inaccurate data. And as already noted, non-EU nationals could not even obtain that.

Moreover, given that only sub-clause (c) refers to "compensatory damages" (as discussed separately below), it seems clear that the judicial body in the US will not be able to award such damages (even to EU citizens) in relation to denial of access or of rectification of incorrect data or "improperly processed" data (other than "unlawfully disclosed" data: see below) – even if the data subject can show actual (material or immaterial) damages resulting from the inaccuracy or improper processing (e.g., from being wrongly labelled a "suspect" or "high risk" on an anti-terrorist watchlist). This is quite unacceptable from a European human rights- and data protection point of view.

The only action in relation to which "compensatory damages" can be awarded by the judicial body is "**wilfully and intentionally unlawfully disclos[ing] information**" relating to

[25] NB: Article 21(2) of the Charter allows for distinctions in treatment on the grounds of nationality, but only to the extent envisaged in the EU Treaties. The relevant provisions in the Treaties relate mainly to voting and residence rights, etc.; they do not allow for discrimination on grounds of nationality in respect of any rights protected by the Charter, and certainly not in relation to the making available of effective remedies and judicial redress.

the data subject seeking redress. This is a very high standard of misconduct. No compensation can be awarded for accidental or even negligent disclosures, even if they result in real, possibly even serious damages. Moreover, from the language it would appear that the wilfulness and intent must extend to the unlawfulness: it is not enough that the defendant agency "wilfully and intentionally" disclosed the data, and that this is held to have been unlawful; rather, the disclosure must wilfully and intentionally (i.e., knowingly) have been unlawful. Again from a European perspective, this is an absurdly high hurdle to ask a complainant to prove.

Article 9(3) suggests that the judicial redress system just discussed (i.e., as set out in Article 19(1) and (2)) is:

> without prejudice to any other judicial review available with respect to the processing of an individual's personal information under the law of the State in which relief is requested.

However, as EPIC has made clear in its Statement to the US House of Representatives Committee on the Judiciary,[26] this does not really provide for any real alternative remedies. In particular, the remedies under the US Privacy Act will in practice not become available, or will only become available to a very limited extent:

> The Judicial Redress Act, as currently drafted, provides only limited opportunities for non-US persons to seek redress under the Privacy Act. First, it limits the scope of the Privacy Act's catchall provision, § 552a(g)(1)(D), to only intentional or willful violations of § 552a(b), which prohibits disclosure of personal information without consent unless the disclosure is subject to the enumerated exceptions. Under the bill, non-US persons will not be able to sue agencies for failure to comply with any other provision of the Privacy Act, nor will they be able to sue for an agency's violation of its own regulations. In addition, a non-US person will only be able to sue a "designated agency" for improper disclosure of her personal information.
>
> Second, the bill substantially limits a non-US person's ability to sue an agency for failure to amend a record or refusal to provide access to a record. According to H.R. 1428, non-US persons will only be able to sue "designated agencies" for refusal to provide access to or for failure to amend a record. Federal agencies that are not "designated agencies" but which maintain records on non-US persons fall outside the scope of the Act's provisions.
>
> Finally, non-US persons have no ground to challenge an agency for an adverse decision—such as a denial of a visa or refugee resettlement application—when the adverse decision resulted from the agency's failure to maintain their records with the requisite accuracy, relevance, timeliness, and completeness necessary for fair determinations.
>
> (p. 3, footnote references omitted)

EPIC therefore rightly argued that the remedy to the non-availability of the Privacy Act remedies to non-US persons should be to simply be to change the definition in that Act of "individual" from meaning only:

> "a citizen of the United States or an alien lawfully admitted for permanent residence" (5 U.S.C. § 552(a)(3)(A))

---

[26] Statement of EPIC on H.R. 1428, the Judicial Redress Act of 2015, 16 September 2015, available at: https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf

(i.e., what is commonly referred to as a "US person") –

to:

"any natural person".

That would also from a European and universal human rights perspective appear to be the only correct step to take.

In sum: Under Article 19, judicial redress is not available at all to any non-EU citizens whose data may have been transferred by EU or EU Member States LEAs to US LEAs; while judicial redress for EU citizens is far too limited. In particular, it would appear that they cannot obtain a judicial order for the deletion or erasure of inaccurate or improperly (indeed, even unlawfully) processed data; and they cannot obtain compensation for damages caused by the information being incorrect, or improperly processed by the US agency. They can only obtain compensation if they can prove actual damages arising from wilfully and intentionally unlawful disclosures of their data by the receiving US agency. This falls far short of an appropriate judicial redress system, such as must be available to "everyone" under the EU Charter of Fundamental Rights.

Article 20: Transparency

1. 1. The Parties shall provide notice to an individual, as to his or her personal information, which notice may be effected by the Competent Authorities through publication of general notices or through actual notice, in a form and at a time provided for by the law applicable to the authority providing notice, with regard to the:

(a) purposes of processing of such information by that authority;

(b) purposes for which the information may be shared with other authorities;

(c) laws or rules under which such processing takes place;

(d) third parties to whom such information is disclosed; and

(e) access, correction or rectification, and redress available.

2. Such notice requirement is subject to the reasonable restrictions under domestic law with respect to the matters set forth in Article 16(2) (a) through (f).

Analysis: It is of course useful if law enforcement agencies make available, through "general notices" – typically, on their websites – the basic parameters of their processing of personal data, including data on foreigners.

More significant is the fact that Article 20(1) specifically refers to "sharing" of personal data received from LEAs of the other party (i.e., as concerns US LEAs, from their EU counterparts) with "other authorities" (Article 20(1)(b)) and to "disclos[ing]" of such personal data to "third parties (Article 20(1)(d)). These separate references must relate to different kinds of recipients of the data – presumably, the "other authorities" with whom the data received from the EU may be "shared" are other authorities in the receiving state, i.e., as concerns EU data transferred to the USA, other US authorities. As noted in the analysis of Article 6(2), above, these appear to include US NSAs to the extent that they can be said to be involved in "the prevention, detection, investigation or prosecution of serious crimes" – which would certainly include the FBI (which, as noted in the analysis of Article 1, is expressly defined as both an LEA and a NSA). The (distinct) "third parties" to whom the data may be disclosed

must then be assumed to be agencies of "third countries", including non-EU countries other than the USA, to which data received from the EU can be "further transferred" subject to Article 7. It could also cover disclosures to private entities, such as perhaps financial institutions (in relation, say, to suspected financial crime) or private-sector contractors.

That aside, the general information listed in Article 20, yet again, falls short of the general information that European controllers are required to make public – if not in the form of general notices, then indirectly, by notifying their national DPA, who then publishes this information, typically in an online-accessible register of controllers. Under Article 19(1) of the 1995 Data Protection Directive, this notification "shall include at least": the following:

> (a) the name and address of the controller and of his representative, if any;
>
> (b) the purpose or purposes of the processing;
>
> (c) a description of the category or categories of data subject and of the data or categories of data relating to them;
>
> (d) the recipients or categories of recipient to whom the data might be disclosed;
>
> (e) proposed transfers of data to third countries;
>
> (f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

The General Data Protection Regulation is likely to add the retention periods of the data to this list.

The possibility of seeking access, rectification, erasure or blocking is of course also widely advertised on the European DPAs' websites.

The main differences between the general information to be made available in the EU and under the Umbrella Agreement are that the latter does not require information to be made publicly available on "the category or categories of data subject and of the data or categories of data relating to them", processed by the US LEA in question, or on "proposed transfers of data [by the receiving US LEA] to third countries". Those are significant differences.

Yet more important are the exceptions to the transparency requirements of Article 20, set out in the second paragraph. This makes clear that the release of the information listed in the first paragraph is subject to "*reasonable restrictions under domestic law*" "with respect to" the following matters (listed in Article 16(2)(a) – (f)):

> (a) protect[ing] the rights and freedoms of others, including their privacy;
>
> (b) safeguard[ing] public and national security;
>
> (c) protect[ing] law enforcement sensitive information;
>
> (d) avoid[ing] obstructing official or legal inquiries, investigations or proceedings;
>
> (e) avoid[ing] prejudicing the prevention, detection, investigation or prosecution of criminal offenses or the execution of criminal penalties;
>
> (f) otherwise protect[ing] interests provided for in legislation regarding freedom of information and public access to documents.

We have already discussed these "matters" in our analysis of Article 16, above. There, we concluded that the US test of "reasonableness" falls far short of the European-constitutional standards of "necessity" and "proportionality".

As drafted, Article 20 of the Umbrella Agreement appears to allow US domestic law to stipulate that any of the matters listed in Article 20(1) shall not be made public, as long as such a restriction on transparency is "*reasonable*" in US-domestic-legal terms. Given the sweeping exceptions and exemptions from the normal rules, already provided for in US law for the benefit of "national security" – which is itself excessively widely defined in US law – and for "protecting law enforcement-sensitive information", Article 20(2) appears to be little less than a *carte blanche* for the US legislative authorities to effectively nullify the transparency seemingly provided for by the first paragraph.

Article 21: Effective Oversight

1. The Parties shall have in place one or more public oversight authorities that:

(a) exercise independent oversight functions and powers, including review, investigation and intervention, where appropriate on their own initiative;

(b) have the power to accept and act upon complaints made by individuals relating to the measures implementing this Agreement; and

(c) have the power to refer violations of law related to this Agreement for prosecution or disciplinary action when appropriate.

2. The European Union shall provide for oversight under this Article through its data protection authorities and those of the Member States.

3. The United States shall provide for oversight under this Article cumulatively through more than one authority, which may include, *inter alia*, inspectors general, chief privacy officers, government accountability offices, privacy and civil liberties oversight boards, and other applicable executive and legislative privacy or civil liberties review bodies.

Analysis: In Europe – but increasingly also elsewhere – "effective oversight" is regarded as an absolutely essential element of adequate data protection; and this provision is thus crucial to any assessment of whether the Umbrella Agreement meets European standards. Shortly after the coming into force of the 1995 Data Protection Directive in 1998, the "Article 29 Working Party" (WP29) already stressed that, in Europe:[27]

> There is ... broad agreement that a system of '***external* supervision**' in the form of an ***independent* authority** is **a *necessary feature* of a data protection compliance system**.

However, it noted that:

> Elsewhere in the world ... these features are not always present.

At that time (in 1998), the WP29 was therefore still flexible in this regard. It was willing to accept a supervisory system in a third (i.e., non-EU) country as "adequate", as long as it "deliver[ed] a good level of compliance with the rules"; "provide[d] support and help to

[27] Working Document – Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive (WP12), adopted by the Working Party on 24 July 1998, p. 7, emphases added.

individual data subjects in the exercise of their rights, in particular also through "some sort of institutional mechanism allowing independent investigation of complaints"; and "provide[d] appropriate redress to the injured party where rules are not complied with. It stressed that the latter requirement (appropriate redress) was:

> a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.

In other words, even then, the independence of the relevant supervisory body and its powers to carry out its own, full and independent investigations, were regarded as key requirements.

Since then, these elements have if been very considerably strengthened in European data protection law. Thus, in 2001, the Council of Europe adopted an Additional Protocol to its Data Protection Convention – which is still the leading global instrument in this field – specifically also to require fully independent supervisory authorities in the State Parties to the Convention and to the Protocol.[28] This stipulates the following in Article 1:

> **Article 1 – Supervisory authorities**
>
> 1. Each Party shall provide for one **or more authorities** to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.
>
> 2. a. To this end, the said authorities shall have, in particular, **powers of investigation and intervention**, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.
>
> b. **Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.**
>
> **3. The supervisory authorities shall exercise their functions in complete independence.**
>
> 4. Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.
>
> 5. In accordance with the provisions of Chapter IV, and without prejudice to the provisions of Article 13 of the Convention, the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.
>
> (Emphases added)

Moreover, in December 2007, the revised EU Charter of Fundamental Rights was adopted, which expressly enshrined data protection as an independent, *sui generis* fundamental right in the EU. Since the coming into force of the Lisbon Treaty two years later, the Charter is furthermore part of the binding law of the Union. This too stresses that independent supervisory authorities with powers to "control" – i.e., in EU parlance, to effectively

[28] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, Strasbourg, 8 November2001, ETS 181.

supervise – the relevant processing, are an essential requirement for any data protection regime that wants to meet the EU's fundamental rights standards:

> Article 8
>
> **Protection of personal data**
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
> 3. **Compliance with these rules shall be subject to control by an independent authority.**
>
> (Emphasis of the last paragraph added)

"Control" in the last paragraph refers to actual powers of investigation and direction.

In European human rights law, "independence" has been interpreted in relation to various "tribunals" and institutions as requiring a "manner of appointment" of the members of the supervisory body, and a term of office that is sufficiently long, to ensure that they are not subject to outside pressures (in particular of course, from the Executive and/or the bodies they are supposed to supervise), and as also requiring that the supervisory body presents "an appearance of independence" to an objective outside observer.[29] This is reflected in the Explanatory Memorandum to the Additional Protocol to the COE Data Protection Convention, as follows:[30]

> Supervisory authorities cannot effectively safeguard individual rights and freedoms unless they exercise their functions in complete independence.[31] A number of elements contribute to safeguarding the independence of the supervisory authority in the exercise of its functions. These could include the composition of the authority, the method for appointing its members, the duration of exercise and conditions of cessation of their functions, the allocation of sufficient resources to the authority or the adoption of decisions without being subject to external orders or injunctions.

---

[29] Cf. e.g, the summary (there in the context of civil law adjudications) in the European Court of Human Rights' Guidance on Article 6 – Fair Trial (civil limb), available at: http://www.echr.coe.int/Documents/Guide_Art_6_ENG.pdf
For the comparable standards in relation to criminal procedures, see the Council of Europe Guide to the implementation of Article 6 of the European Convention on Human Rights, Human Rights Handbook No. 3, p. 30ff., by Nuala Mole and Catharina Harby, available at: http://www.echr.coe.int/LibraryDocs/DG2/HRHAND/DG2-EN-HRHAND-03(2006).pdf

[30] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, Strasbourg, 8 November2001, *Explanatory Memorandum*, para. 17, available at: http://conventions.coe.int/Treaty/EN/Reports/Html/181.htm

[31] In respect of the procedural guarantees set forth in Article 8 of the European Convention on Human Rights, the case law of the organs of this Convention already considers the intervention of an independent body, in certain circumstances, as a guarantee of "effective supervision" of the need for an interference by a public authority with the exercise of the rights provided by Article 8 (cf *Gaskin vs United Kingdom*, decision of 7 July 1989, series A no. 160, § 49). [original footnote to the Explanatory Memorandum]

Clarification of the other the key features that define an acceptable type of oversight- or supervisory authority is also provided in the Explanatory Memorandum, as follows:[32]

> Parties have considerable discretion as to the powers which the authorities should be given for carrying out their task. According to the Protocol, however, they must at least be given **powers of investigation and intervention**, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities any violations of the relevant provisions.
>
> The authority shall be endowed with powers of **investigation**, such as the possibility to ask the controller for information concerning the processing of personal data and to obtain it. Such information should be accessible [to the relevant supervisory authority] in particular when the supervisory authority is approached by a person wishing to exercise the rights provided for in domestic law, by virtue of Article 8 of the Convention.
>
> The supervisory authority's power of **intervention** may take various forms in domestic law. For example, the authority could be empowered to ***oblige*** the controller of the file to rectify, delete or destroy inaccurate or illegally collected data on its own account or if the data subject is not able to exercise these rights himself/herself. The power to ***issue injunctions*** on controllers who are unwilling to communicate the required information within a reasonable time would be a particularly effective manifestation of the power of intervention. The supervisory authority should have the power to inform the public through regular reports, the publication of opinions or any other means of communication.
>
> ...
>
> The Parties should give to the supervisory authority the power either to engage in legal proceedings or to bring any violations of data protection rules to the attention of the judicial authorities. This power derives in particular from **the power to carry out investigations, which may lead the authority to discover an infringement** of a person's right to protection. The Parties may fulfil the obligation to grant this power to the authority by enabling it to make judgments.

Although it is clear from the text of the Additional Protocol and the Explanatory Memorandum that there could, in any State Party to the Convention and the Protocol, be more than one supervisory authority, the suggestion in these texts is strongly that within any one particular area of competence there should be one such authority with all the powers of investigation and intervention mentioned. Thus, there could be separate authorities for supervision over controllers in the public or private sectors, or within federal states, over controllers in different states, or (as is the case in several EU MSs) a separate supervisory authority over processing of personal data by law enforcement agencies.

However, the Umbrella Agreement stipulates that in the USA "effective oversight" over the processing by US LEAs of the personal data provided to them by EU LEAs subject to the Umbrella Agreement can be provided:

> cumulatively through more than one authority, which may include, *inter alia*, inspectors general, chief privacy officers, government accountability offices, privacy and civil liberties oversight boards, and other applicable executive and legislative privacy or civil liberties review bodies.

[32] Additional Protocol (previous footnote), paras. 11 – 13 and 15, emphasis added, footnote omitted.

It is impossible within the scope of this Annex to analyse all the possible officers, offices, boards and other bodies in the USA to which this could possibly apply. The Umbrella Agreement does not even list them. But was is clear is that there are, in the USA, no single bodies that combine in themselves the requirements of independence and powers of investigation and intervention that are seen as key to the adequacy of European supervisory authorities. Some do not have jurisdiction in respect of much of the processing. Some may have the right to raise questions, perhaps also on behalf of data subjects – but without being given the right to investigate independently, with full access to all the relevant data (even if not all may be revealed to the complaining data subjects). Some may be able to make recommendations in respect of corrections or additions or other "remedial actions" – but as far as we know, none can *order* such changes. What is more, as discussed in the analyses of Articles 17 and 18, above, US law and practice generally appears to never consider compulsory deletion of data – even of data proven to be incorrect or improperly, or even unlawfully, processed – to be mandatory; and none of the US officers, bodies, etc., that could possibly be regarded as falling within the list in Article 21(3) will, as far as we can see, ever be able to order it. Moreover, the Article does not specify exactly which aspects of data protection law it refers to.

In our view, the oversight offered in this article on the US side falls far short of the minimum European requirements for "independent [supervisory] authorities", enshrined in the Additional Protocol to the COE Data Protection Convention or, what is more, in the EU Charter of Fundamental Rights.

Given that in, Europe, oversight by such truly independent and fully empowered authorities is seen as crucial to adequate protection and as constitutionally required, the absence of serious guarantees to that effect in the Umbrella Agreement again raise serious doubts about its validity in terms of the Charter and EU law.

Article 22: <u>Cooperation between oversight authorities</u>

1. Consultations between authorities conducting oversight under Article 21 shall take place as appropriate with respect to carrying out the functions in relation to this Agreement, with a view towards ensuring effective implementation of the provisions of Articles 16, 1 7, and 18.

2. The Parties shall establish national contact points that will assist with the identification of the oversight authority to be addressed in a particular case.

<u>Analysis</u>: "Cooperation" between data protection oversight bodies is of course crucial in relation to transnational processing of personal data and the transfer of personal data from the jurisdiction of one such body to the jurisdiction of another one, especially if they are in different countries. The new General Data Protection Regulation makes extensive provision for much extended cooperation of this kind, including "mutual assistance" – which can include exercising inspection etc. powers on behalf of another authority; and "joint operations".[33] However, in spite of the use of the word "cooperation" in the heading, the Umbrella Agreement envisages nothing of the sort.

Rather, as already noted in the analyses of the articles in the Umbrella Agreement on the exercise of data subjects' rights of access and rectification (Articles 16 and 17), the European

[33] See the GDPR, Chapter VII, Section 1 – Co-operation (Articles 55 and 56).

DPAs are basically treated as no more than a representative of the data subjects. They cannot themselves investigate any issues relating to any data transferred to the USA subject to the Umbrella Agreement, and they certainly have no powers to "intervene" with the US receiving authorities in the sense in which that word is used in Europe, i.e., to direct those authorities to do or refrain from doing anything.

That might in itself be acceptable, if the "cooperation" between the European DPAs and the (miscellaneous and dispersed) US supervisory authorities could amount to anything resembling the cooperation between DPAs envisaged in the GDPR, i.e., if the European DPAs could – especially when acting on behalf of European data subjects, but also more generally – *demand* that the relevant US supervisory authorities carry out full and proper investigations, with full access to all the data at issue, and "intervene" as appropriate, i.e., if the latter has powers to *order* remedial action, also at the behest of their European counterparts.

But the Umbrella Agreement offers nothing of the sort. First of all, Article 22(1) only refers to "consultations" between the European and the US supervisory authorities, "with a view towards ensuring effective implementation of the provisions of Articles 16, 1 7, and 18", i.e., the effective implementation of subject access and rectification (insofar as provided for in the US legal framework, which as we have seen is not very far) and the offering of "administrative redress" (which we have seen is actually pretty meaningless). These "consultations" may have those (limited) aims, but the Agreement does not provide anything to guarantee that even these limited aims are achieved.

Given the complexity and ill-defined nature of the myriad of US officers, bodies, etc., that might be called upon in these contexts, each with different mandates and powers, perhaps the second paragraph of Article 22 is the most useful: it requires the Parties to the Agreement – i.e., the EU, the USA, and in effect the EU Member States – to:

> establish national contact points that will assist with the identification of the oversight authority to be addressed in a particular case.

But overall, Article 22 does not ensure cooperation between the EU and US authorities that can result in real, effective, binding enforcement of the principles in the Agreement against the receiving US LEAs. More in particular, the European DPAs have no formal standing in that regard at all.

Article 23: Joint Review

1. The Parties shall conduct periodic joint reviews of the policies and procedures that implement this Agreement and of their effectiveness. Particular attention in the joint reviews shall be paid to the effective implementation of the protections under Article 14 on accountability, Article 16 on access, Article 17 on rectification, Article 18 on administrative redress, and Article 19 on judicial redress.

2. The first joint review shall be conducted no later than three years from the date of entry into force of this Agreement and thereafter on a regular basis. The Parties shall jointly determine in advance the modalities and terms thereof and shall communicate to each other the composition of their respective delegations, which shall include representatives of the public oversight authorities referred to in Article 21 on effective oversight, and of law enforcement and justice authorities. The findings of the joint review will be made public.

3. Where the Parties or the United States and a Member State have concluded another agreement, the subject matter of which is also within the scope of this Agreement, which provides for joint reviews, such joint reviews shall not be duplicated and, to the extent relevant, their findings shall be made part of the findings of the joint review of this Agreement.

Analysis: As will be clear by now, we believe that the Umbrella Agreement should not be adopted in its current form at all. But if it is (perhaps with changes or with additional, separate guarantees and assurances), it still touches on such delicate issues affecting the fundamental rights of European data subjects that it should be made subject to a "sun-set clause", after which it automatically expires unless the parties agree to renew it, perhaps with amendments. In our view, the initial period suggested – three years – is also too long; it should be no more than two years at most.

Moreover, any review should not be restricted to certain specified – and thus, by that specification, limited – issues, i.e., as suggested in paragraph (1), to:

> the effective implementation of the protections under Article 14 on accountability, Article 16 on access, Article 17 on rectification, Article 18 on administrative redress, and Article 19 on judicial redress.

We note in particular that the very problematic provisions on "sharing" data with "other authorities" (Article 6(3)) and "onward transfer" of received data to "third parties", presumably in third countries (Article 7), are not included in the above. Since, in our view, they are amongst the most problematic of the provisions in the Umbrella Agreement, their implementation in practice should most certainly be reviewed. Answers should be given to the question of whether, if further disclosures of transferred data to NSAs in the USA and elsewhere are indeed possible under the Agreement (as we believe they are), they actually occurred; who the end-recipients were; and whether any of the EU-provided LEA data have ended up in the UKUSA/5EYES (*et al.*) global surveillance programmes.

Also crucial would be that such a review would be conducted completely openly and transparently, presented to the public as well as national and EU parliaments and other authorities, with full access to and disclosure of the facts on how the Agreement operates to both the European Parliament and the general public. It was already scandalous that such an important agreement was effectively negotiated in secret. It should certainly not be reviewed and further extended in secrecy (or quasi-secrecy). Merely publishing the "findings" of the review, as is suggested in paragraph (2) is not good enough.

The third paragraph is also puzzling. It stipulates that if there are any other agreements between the EU and the USA, or between the USA and any EU MS, to which the Umbrella Agreement will apply (i.e., that relate to transfers of data [also?] for law enforcement purposes, and that provide for reviews of their operation, the latter reviews would be subsumed in the – as we have just seen, limited and largely closed – reviews provided for in Article 23. This could apply, for instance, the the EU-US MLAT of 2003, to the EU-US PNR Agreement, and indeed to all sorts of agreements between the USA and EU MSs.

To simply abandon all such other specific reviews of the operation of all such other specific agreements, and to replace them with the inadequate review provided for here is once again unacceptable from a European human rights- and data protection perspective.

Article 24: Notification

1. **The United States shall notify the European Union of any designation made by U.S. authorities in relation to Article 19, and any modifications thereto.**

2. **The Parties shall make reasonable efforts to notify each other regarding the enactment of any laws or the adoption of regulations that materially affect the implementation of this Agreement, where feasible before they become effective.**

Analysis: The first paragraph refers to notification by the USA of the adoption, as and when this happens, of the Judicial Redress Act, mentioned in the Introduction to main Note. As explained there, the Umbrella Agreement will not be ratified by the EU until this has happened.

The second paragraph suggests that the EU and the USA could enact laws and adopt regulations that "materially affect the implementation of [the Umbrella Agreement]" and bring these into effect, without first notifying the other party (or the EU MSs) if such notification is not "feasible". It is difficult to imagine laws and regulations with such significant impact – on the relations between the parties, not to mention the rights of EU data subjects – that have to be enacted or adopted in such a hurry that it is not "feasible" (?!) to inform the other party. There is no justification for this provision.

Article 25: Consultation

Any dispute arising from the interpretation or application of this Agreement shall give rise to consultations between the Parties with a view to reaching a mutually agreeable resolution.

Analysis: It is notable that this is the only provision relating to resolving disputes about "the interpretation or application of [the Umbrella Agreement]". Surely, such legal matters should be resolved in a judicial forum? In particular, this would appear to be yet another attempt in the Agreement to sideline any possibility of the CJEU, or any national (constitutional) court ruling on the meaning – and constitutional acceptability – of the Agreement (or of the way it is interpreted or applied).

As it stands, the only option for a party which seriously objects to an "interpretation or application" of any of the provisions of the Agreement by the other party, but who cannot convince the other party to change its interpretation or practices, would be to use the very heavy option of suspending or terminating the Agreement, in accordance with Article 26 or 28, as appropriate.

Article 26: Suspension

1. **In the event of a material breach of this Agreement, either Party may suspend this Agreement in whole or in part by written notification to the other Party through diplomatic channels. Such written notification shall not be made until after the Parties have engaged in a reasonable period of consultation without reaching a resolution and suspension shall take effect twenty days from the date of receipt of such notification. Such suspension may be lifted by the suspending Party upon written notification to the other Party. The suspension shall be lifted immediately upon receipt of such notification.**

2. **Notwithstanding any suspension of this Agreement, personal data falling within the scope of this Agreement and transferred prior to its suspension shall continue to be processed in accordance with this Agreement.**

Analysis: It should be noted that this provision does not deal with possible or suspected breaches of the Agreement, about which one could argue: those are subject to Article 25 rather than to Article 26. Nor does it concern trivial breaches. Rather, it deals with *established, material breaches* of the Agreement by one of the parties. It is notable that even in such egregious cases, the injured party is not allowed to suspend the operation of the Agreement with immediate effect; and that the party that caused the breach can, for some weeks, continue to process personal data falling within the scope of the Agreement and transferred prior to its suspension (but possible still after the notification to that party of the fact that its actions are in "material breach" of the Agreement. That appears to us to be over-generous to the wrong-doer. Anyway, it is hard to see how the material breach can be proved in the absence of an effective inspection process.

Article 27: Territorial application

1. **This Agreement shall only apply to Denmark, the United Kingdom, or Ireland if the European Commission notifies the United States in writing that Denmark, the United Kingdom, or Ireland has decided that this Agreement applies to its State.**
2. **If the European Commission notifies the United States before the entry into force of this Agreement that this Agreement will apply to Denmark, the United Kingdom, or Ireland, this Agreement shall apply to such States from the date of entry into force of this Agreement.**
3. **If the European Commission notifies the United States after the entry into force of this Agreement that it applies to Denmark, the United Kingdom, or Ireland, this Agreement shall apply to such State on the first day of the month following receipt of the notification by the United States.**

Analysis: This article speaks for itself. Suffice it to reiterate what was already noted in the analysis of Article 19: that ironically, until and unless Denmark, the UK and Ireland join the Umbrella Agreement in accordance with this Article 27, their citizens will be completely denied judicial redress in the USA under the Agreement (in the same way as it is denied to refugees etc. in the EU) – in violation of the Charter.

Moreover, this provision appears to assume that the legal basis for the treaty is Article 87 TFEU (police cooperation, including exchange of personal data), which gives these States an opt-out; but in fact it is arguable that the sole or joint legal base is Article 16 TFEU, concerning data protection law, from which there are no opt-outs.

Article 28: Duration of the Agreement

This Agreement is concluded for an unlimited duration.

Analysis: As already mentioned in our analysis of Article 23, above, we believe that the Umbrella Agreement should not be adopted in its current form at all, but if it is, it should be made subject to a "sun-set clause" of no more than two years at most.

Article 29: Entry into force and Termination

1. **This Agreement shall enter into force on the first day of the month following the date on which the Parties have exchanged notifications indicating that they have completed their internal procedures for entry into force.**

2. Either Party may terminate this Agreement by written notification to the other Party through diplomatic channels. Such termination shall take effect thirty days from the date of receipt of such notification.

3. Notwithstanding any termination of this Agreement, personal information falling within the scope of this Agreement and transferred prior to its termination shall continue to be processed in accordance with this Agreement.

Analysis: The first two paragraphs are standard in international agreements. The final paragraph could be problematic, if the Agreement were to be terminated by one party (say, the EU) because it believed the other party (say, the USA) was acting in "material breach" of the Agreement (cf. Article 26), but that other party disagreed; and the matter could not be resolved in the "consultations" envisaged in Article 25. To allow the second party to continue to process the data transferred to it under the Agreement in a way that the other party regards as seriously in violation of the Agreement is wrong. There should be arrangements for judicial international settlement of such matters.

- o – O – o -

Douwe Korff

Cambridge, September-October 2015