

EU Public Consultation on the Future EU – US International Agreement on Personal Data Protection and Information Sharing for Law Enforcement Purposes



On behalf of

European Privacy Association (ABSL)

Square de Meeus, 37 - 4th Floor

1000 Brussels, Belgium

Register ID number: 97050032046-57

info@europeanprivacy.eu – www.europeanprivacy.eu

Contribution by *Marco R. Provierera, Member of the Scientific Committee of the European Privacy Association*

Submitted by *Luca Bolognini – Executive board European Privacy Association*

Answers to the Consultation Questionnaire

1. Purpose

The major macro-development, which has taken place subsequently to the High Level Contact Group (HLCG) submission of the Final Report of May 2008 was with no doubt the entry into force of the Lisbon Treaty. It is uncertain whether the Addendum to the Report of October, 2009, took such EU crucial institutional change in all due account as per a sound looking-forward perspective – under Lisbon Treaty, Article 16, by 2014 the “pillar” structure will no longer exist and there will be one legal basis for data protection within the EU – or the policy choice was to keep the envisaged EU-US Agreement under the pillar-based old legal framework. In the latter hypothetical, as pointed out in the 2008 Opinion of the EDPS (II.13), some legal uncertainty “about the dividing line between the pillars” would persist, in that the Agreement would seem to squarely fall into the third pillar, thus into the applicability-excluding “first pillar” provisions of the Directive 95/46/EC¹.

Absent clarifications on this fundamental issue, it is our view that the existing instruments background² allows the argument that a legally binding agreement, in close coordination with such existing instruments, should clearly specify and circumscribe the covered areas under the wide “law enforcement” definition, including mutual information transfers criteria, and impact on relations with other third countries, according to the basic principles of relevance, necessity and proportionality³, but also in view of the marked need of an enhanced and effective cooperation EU-US in the fields of national/international security and law enforcement.

¹ Directive 46/95/EC, Considerata 13, 35, 43; But also 21, 45, 56.

² Namely, the previous EU-US 2002 Europol, 2003 Extradition and Mutual Legal Assistance, and 2006 Eurojust agreements, together with the 2007 PNR agreement and the 2007 SWIFT-related exchange of letters on the Terrorist Finance Tracking Program.

³ EDPS Opinion, 2008, V.1.58, at 13.

2. Scope of the Agreement

2.1 Material Scope

As pointedly recalled by the EDPS Opinion⁴, “[T]he issue of transfer of personal data to third countries in the framework of police and judicial cooperation in criminal matters is addressed in the “Council Framework Decision on the protection processed in the framework of police and judicial cooperation in criminal matters” of 2008.

Hence, careful coordination should be sought between this pre-existing instrument and any Agreement’s provision, in order to avoid overlaps, possibly adding to confusion, under the newly-enforced Treaty on the Functioning of the European Union (TFEU), Title V, chapter 5, and Title V, chapter 4.

While any reference to, and thus any inclusion in the Agreement’s scope of, matters concerning civil law cooperation do not seem to fit the Agreement core purposes – also given the number of existing instruments and on-going multi-lateral, as well as transatlantic, cooperation efforts in the civil law area – this commentator shares the EDPS view that, as concerns the first pillar immigration, visa and asylum issues, strict compliance is needed with the proportionality, necessity, reciprocity principles, together with “[A] circumscribed scope of application, with a clear and common definition of law enforcement purposes at stake”⁵, on a exchange of data case-by-case basis.

2.2 Personal Scope

On this issue, this contribution profoundly differs from the EDPS’ highly reluctant stance on the applicability of the Agreement to data transfers between “private and public actors”.

In fact, while rule of law and due process fundamental principles obviously require clear spelling out and consistency of specific instances and circumstances where obligations to

⁴ Ibidem, I.7, at 2.

⁵ Ibidem, VI.82, at 17.

provide data should be imposed on private entities, both harsh realities and recent history of the major threats to transatlantic security – namely terrorism and organized crime – leave no doubt that, especially in the today’s “information society”, failure to establish provisions on private entities-law enforcement authorities exchanges of data would jeopardize the very central purpose of the Agreement. Both the collection of so-called PNR data from airlines and the SWIFT program proved to be invaluable tools not only in the context of thoroughly fighting the terrorism, but also, specifically, and in a crucial number of instances of prevention/prosecution of serious transnational crimes and/or acts of terrorism.

Therefore, so-called “bulk transfers” of data in specific sectors – commercial flights and financial transactions in chief – appear to be inevitable, if perhaps unappealing in an ideal world, and the Agreement should realistically spell out specific conditions and limits in order to provide reasonable guarantees to data subjects without depriving authorities of necessary tools to ensure common security.

Yet, in reference with the data exchange between public authorities, we concur with some of the EDPS sound concerns with regards to the needed clarifications on whether: a) the Agreement would aim at centralized or decentralized (Member States managed) database; b) tax databases would be included; c) a case-by-case-transfer approach would be preferable rather permanent access to existing databases; A further sensitive issue is whether national security agencies would have direct access to law-enforcement databases under the other contracting party’s control: while strict cooperation between national security agencies, as well as operational effectiveness, are crucial, nevertheless some incremental-clearance-based-process steps to mutual access are to be envisaged.

3. Nature of the Agreement

The reciprocity requirement, or mutual recognition, at first glance of no contention, entails, under closer scrutiny, a number of sensitive considerations on legal systems differences, and consequent need to strive to find workable compromise.

While there doesn't seem to be question about the reciprocity of access, with the above-mentioned guarantees, by law enforcement authorities to same type/category of personal data, both the "adequate level of protection" standard and the redress issue have proven to be among the most difficult – seemingly almost intractable as per the "redress" conundrum – to come to terms with⁶.

The "adequacy" test, while taking into consideration experiences in different areas, should be applied, in the context of the Agreement, in a more flexible way than under the Directive 95/46/EC, Art. 25 regime for transfer of data to third countries, consistently with the Agreement inherent third pillar nature⁷. We will further discuss the redress issue below, at 4.4.

⁶ Redress was still, after two-year long bilateral negotiations, defined as an "outstanding issue" in the 2008 HLCG Report, 2.5, at 5; the 2009 Annex to the Addendum could only reiterate, in general terms, the necessity to provide for individuals' effective remedies "before an impartial, competent authority".

⁷ As to take into account, in a constructive way, the historical and current differences between legal systems and government structures; we agree that some invaluable guidance may be provided by principles set forth in the U.N. Guidelines, Convention 108 of the Council of Europe and the OECD Guidelines.

4. Data Protection Principles

4.1 Accountability

Accountability has been specifically recognized, in the 2008 HLCG Report as one of the “Agreed upon Principles”⁸ of the forthcoming Agreement.

For such purpose, including a joint review mechanism might be decisive to ensure full compliance.

4.2 Individual Access

Such joint review body, while fully separated from, and hopefully not overlapping with, ordinary judicial review, would also serve the purpose to indirectly verify and assure proper oversight on instances where individual access to personal data being processed and possibly transferred under the Agreement would not be compatible with on-going investigations need to confidentiality.

Although such individual right of access cannot, in fact, resemble in nature to that provided for in Directive 95/46/EC⁹, the Agreement should nonetheless clearly spell out the extent of said individual right, its limits and proper safeguards, together with enumerating and defining instances where objections to processing/transferring of data are, or are not, allowed.

Since we harbour some perplexities on the simplistic transposition of the EU-type data national authorities model at any international level – given, pointedly, accountability and judicial review issues that such approach would carry -

4.3 Single Contacts Points

⁸ HLCG Report, 2.B, at 4.

⁹ While some comparative guidance may well be provided by safeguard principles embodied in Directive 06/24/EC.

Given both the complexity of the US framework for privacy protection and the number of EU Member States data protection authorities, an approach based on the Agreement binding, treaty-like authority, to establish jurisdictional-concern-free two single-contact points – one in the US for data protection concerns related to data transferred from the EU, and one in the EU for concerns over data transferred from the US – appears to be a promisingly workable solution.

Since we are never too often reminded that we are addressing issues related to a law-enforcement/security context, and hence strict principles of rule of law and due process must fully govern applicable provisions, the Agreement should clearly spell out powers, limits and accountability of such “contact points”, as well as defining their nature as administrative bodies.

4.4 Judicial Redress

The Questionnaire’s two relevant questions highlight those which seem to be the core difficulties of a coordinated approach to this fundamental intersection of the envisaged Agreement.

The 2008 EDPS Opinion’s analysis¹⁰ must be praised for reiterating well-settled EU principles and “constitutional traditions common to member States” on the basic availability of “a judicial remedy” for redress.

However, the very same Opinion seems to fall short, by plainly emphasizing the EU-style data protection authority solution, to fully appreciate both the shortcomings of such solution’s international applicability and the complex issues raised by a simplified approach, attempting to automatically transpose European views on the interplay of administrative and judicial remedies to the US common-law-based legal system.

Yet, the 2008 HLCG Report accurately and soundly summarizes the fundamental differences of “[T]he US framework for privacy protection...from a networked and layered

¹⁰ EDPS Opinion, V.10.75-77, at 16.

set of authorities arising from the common law and specific protections guaranteed under the US Constitution.”¹¹.

Not only, in fact, as accurately reminded by the Report’s analysis, the US Constitution separation of powers doctrine, under which judicial review of administrative/executive power acts may take place only once remedies in nature administrative have been exhausted, seems to prevent subjects not specifically entitled under federal law¹² from automatic access to the US federal court system, but also does same prevention seem to be dictated on compelling “federalist” grounds¹³. No international agreement presenting constitutional issues would obtain US Senate consent for ratification, and subsequent domestic implementation.

While the HLCG Report meritoriously strives to diplomatically word such fundamental legal traditions’ differences, conceding that both systems ensure “the availability of ‘appropriate and effective sanctions and/or remedies’ as defined...”, it appears to this commentator that the crucial impasse may be overcome only through allowing data subjects, perhaps on a revised, more liberal and extended basis, though still minding that the context is a law-enforcement/security scenario, to seek judicial redress in the data originating jurisdiction, i.e. their own jurisdiction¹⁴, with all their original safeguards.

Such approach, which, in addition, would be much more consistent with a third-pillar scenario, would effectively assure actual and reasonable access to judicial review; cross-jurisdictional implementation and effectiveness of remedies/sanctions would be achieved through existing or novel instruments resembling mechanisms of existing private international law, e.g. conventions on mutual judicial recognition, etc., not mentioning, last but definitely not least, that aggrieved data subjects would be spared the grave

¹¹ 2008 HLCG Report, 2.C, at 6.

¹² Whether, among others, related to the “sectoral” privacy protections, the 1974 Privacy Act – seminal statute governing US citizens and permanent residents’ individual rights related to government-controlled or processed data – the 1984 Computer Fraud and Abuse Act, the 1994 Communications Assistance for Law Enforcement Act, or the 2002 E-Government Act, from a public law viewpoint, or the Federal Trade Commission Act, from an administrative, consumer-oriented viewpoint. Furthermore, some exclusions of aliens’ possibility to avail themselves of the US court system may be grounded, inter alia, on complex personal jurisdiction doctrines.

¹³ Here, reference should be made to the venerable tradition of distinction between “constitutional” privacy – when a government entity is involved – and “private” privacy – attaining to private intrusion – in the US legal tradition, in order to account for State courts jurisdiction (as opposed to federal courts’) to hear grievances of tort liability for violation of the private right to privacy.

¹⁴ It is, in fact, the data subject’s very jurisdiction to be held ultimately liable for the alleged mishandling of data, or for allowing (here’s why other contracting party agencies’ direct access to databases is not advisable) such alleged mishandling.

burden/inconveniences – and presumably high costs – inherent to endeavouring to seek judicial redress in a foreign jurisdiction, governed by a non-familiar legal system.

5. Other Comments

1. Timing

Terrorism and serious transnational crime amount to clear and present danger for transatlantic security and economic prosperity, all the more for EU and US citizens' general freedom and quality of life.

In our democratic societies, founded on the rule of law, these evils must be vigorously fought in accordance with fundamental principles of legal certainty and international cooperation.

A comprehensive Agreement, built on the invaluable work set forth in the 2008 HLCG Report and 2009 Annex to the Addendum – enriched by top-level bilateral contributions, like the pointed and dissecting, in-depth analysis provided by the 2008 EDPS Opinion – and enshrining fundamental transatlantic cooperation principles, is long due and no longer to be postponed.

While, in 2008, concerns related to the still evolving EU institutional framework might have been justified, for purposes of cautiously addressing the issue, today, after the Lisbon Treaty has entered into force, a mutually satisfactory Agreement should be expeditiously attainable and its completion should be promptly and decisively pursued.

2. Troubling News for Sound Approach to Privacy/Security Issues

In spite of top European leaders' advice, as well as urges, based on detailed explanatory reports, from US top national security advisors and last-minute pleas by such high-ranking US officials as Vice-President Biden and Secretary of State Clinton, as of February 11, the EU Parliament rejected the 9-months extension of the SWIFT program on exchange of financial information, within the Terrorist Finance Tracking Program (TFTP). As the Obama administration rightly put it, this was "a setback for US-EU counter terror cooperation".

If the EU Parliament, in the infancy of its new powers under the Lisbon Treaty – which, however, must be hailed for the finally democratic structure it establishes for the EU

institutional framework – intended to send a message that it is ready and willing to exercise such powers, we are not shying away from arguing that jeopardizing the US-EU cooperation efforts in this highly sensitive area showed a worrying view of the privacy/security legal state of the play.

The whole applicable body of privacy law, in both legal systems and under the great human rights conventions and other instruments of international law, make it clear that, in the realms of criminal law enforcement and national/international security, only rule-of-law and due-process guarantees and safeguards apply to protect inalienable individual rights, together with general principles of proportionality, relevancy and necessity.

Security is, in fact, a fundamental commonly-accepted constitutional tenet and, when interfering, or allegedly at odds, with the right to privacy, collision should be avoided through careful balancing analysis and not improperly and out-of-context applying the data protection laws, whose scope has been consistently circumscribed to non-penal application and reach.

The recent privacy-related concerns about body scanners deployment in European airports reflect the same misdirected understanding of privacy law: arguably those security devices do not, in fact, entail anything like a potentially illegitimate processing of personal/sensitive data – specially belonging to fully consenting and aware subjects – leaving alone the clear flaws of an approach which fails to recognize the trade-off between a TC-scan like, anonymous check and the attempt to avert deadly threats to commercial flights safety.

Rome, March 10, 2010