Counterterrorism and Humanitarian Engagement Project

Implications of the USAID Partner Vetting System and State Department Risk Analysis and Management System under European Union and United Kingdom Data Protection and Privacy Law

Neal Cohen
Robert Hasty
Ashley Winton

Research and Policy Paper

March 2014

Neal Cohen is an Associate and Ashley Winton is a Partner in the London, England, UK offices of White & Case L.L.P. Robert Hasty is a Counsel in the Washington, D.C., U.S.A. offices of White & Case L.L.P. The views and opinions expressed in this paper are solely those of the authors. This paper does not constitute legal advice and may not be relied upon as such, nor does it act to create an attorney-client relationship. It should not be acted upon in any specific situation without appropriate legal advice. White & Case L.L.P. has no responsibility for the content of this paper and does not endorse the information, content, presentation, or accuracy, or make any warranty, express or implied.

This publication is part of a research and policy project and reflects research carried out by the authors. The opinions expressed in this paper do not necessarily reflect the views of the Counterterrorism and Humanitarian Engagement Project.

Suggested citation:
Neal Cohen, Robert Hasty, and Ashley Winton, "Implications of the USAID Partner Vetting System and State Department Risk Analysis and Management System under European Union and United Kingdom Data Protection and Privacy Law," Counterterrorism and Humanitarian Engagement Project, *Research and Policy Paper*, March 2014.

The U.S. government has established two anti-terrorist vetting programs aimed at nongovernmental organizations (collectively, "**NGOs**") that are funded by the U.S. government. Under the U.S. Agency for International Development's ("**USAID**") Partner Vetting System ("**PVS**") and the U.S. Department of State's ("**State Department**") Risk Analysis and Management ("**RAM"**) vetting system, any grant awarded to an NGO is subject to the NGO's compliance with the relevant vetting program. However, the PVS and RAM present a conflict with European data protection and privacy law and its national implementations in the Member States.

NGOs which have offices or affiliates in the European Union, or who partner with organizations in the European Union, and who are subject to PVS or RAM are asked to make a decision: whether to comply with the PVS and RAM or, alternatively, to breach European data protection and privacy law. (Please note: the fact that an NGO might also be funded by a European Union Member State does not change the analysis below.)

BACKGROUND

The PVS and RAM are systems for screening individuals involved in administering USAID- and State Department-financed activities or resources, including contracts, grants, and other assistance for the purpose of ensuring U.S. government funds do not flow to entities or individuals deemed to be a risk to U.S. national security.

While the parameters of the PVS and RAM are still unclear in some respects, we understand that as part of the vetting process, NGOs, as applicants for certain USAID or State Department contracts, grants, or other assistance, must in some cases enter the personal data of key personnel and other key individuals for themselves as well as for sub-grantees, sub-contractors, and other partners ("**Partners**") involved in such USAID- or State Department-financed programs into an online governmental portal.[1] Such personal data may include, for example, the name, government-issued photo ID number, social security or passport number, email address, telephone numbers, birth date and place, gender, and in some cases tribal affiliation for such individuals. This personal data is collected by the NGO applicant for both its key personnel and the key individuals of its Partners, and entered by the applicant into the U.S. government portal for screening by the U.S. government against internal U.S. government terrorist databases.

In contrast, in order to apply for a USAID or State Department grant, it is necessary to (i) obtain a Dun & Bradstreet DUNS number and (ii) register with the U.S. System for Award Management.[2]

1. Pursuant to a recent letter, the State Department agreed to offer NGOs an option of "direct vetting", but only for the five (5) grouped pilot countries: Guatemala, Kenya, Lebanon, the Philippines and the Ukraine. Direct vetting is where NGOs put Partners in contact with the State Department so that the Partners may provide personal data directly to the State Department rather than the NGOs providing the Partners' personal data to the US Government. Letter from Patrick F. Kennedy, Under Sec. of State for Management, to Samuel A. Worthington, President and CEO of InterAction (abt Aug. 6, 2013). Afghanistan was expressly excluded (i.e., the NGOs must collect, submit and verify data on key personnel and key individuals, including of subawardees, vendors, etc.). Furthermore, although not clear, a recent Notice of Proposed Rulemaking seemed to indicate that USAID would permit direct vetting for PVS. Partner Vetting in USAID Assistance, xxx Fed. Reg. xxx (August 29, 2013) (*see*, *e.g.*, Proposed Rule 22 C.F.R. pt. 226.92(j)).

2. *See* USAID Grant and Contract process, available at http://www.usaid.gov/work-usaid/get-grant-or-contract/grant-

This requires submitting the NGO's name, address, telephone number, legal structure, date NGO was created, primary purpose of the NGO, total number of employees and name of the NGO's CEO/owner. Other personal data may also be collected in the substantive part of the grant application. The specific additional personal data included will be dependent on the nature of the project. For example, if an NGO is collaborating with Partners, it will reasonably follow that the NGO may need to identify the Partners in the NGO's grant application and provide similar information for the Partners as to what the NGO provided for itself. Yet, the information in the aforementioned example contains only the personal data of the CEO/owner of the NGO and the Partners and not the personal data of key employees and other key individuals. The personal data of the NGO's key employees and other key individuals is not necessary to award a grant and is used solely for vetting purposes, unless otherwise necessary to describe the substance of the project in the grant application.

If the vetting raises concern as to any particular individual, the applicant is notified and the relevant applicant or Partner will in some instances (depending on determinations made by the U.S. government) be disqualified from receiving the award, contract, further orders, etc. As we understand it, the process for an individual whose information has been entered into the portal to access that data or correct his or her data is undefined and there is little assurance that the reasons for a denial will be provided; in at least some cases there may be only a seven (7) day calendar window (at most) to request reconsideration and no right to appeal a finding to any other body or court. In addition, USAID and the State Department may share data on individuals with other U.S. government entities and other governments for reasons that have not been clearly defined.

Below, we have addressed whether NGOs' compliance with the PVS and RAM as currently proposed would represent a conflict of law with European Union ("**EU**") data protection and privacy law and, at times, as implemented in the United Kingdom ("**UK**"), to serve as an example. In this respect, we have addressed:

I. The territorial scope of European data protection and privacy law;

II. Specific requirements of European data protection law which are in conflict with the PVS and RAM;

III. Specific requirements of European data protection and privacy law which are in conflict with the PVS and RAM;

IV. Examples of conflict of laws in relation to European data protection and privacy law;

V. Police and judicial co-operation in criminal matters; and

VI. Penalties and sanctions for violations of UK data protection and privacy law.

and-contract-process; *see also* U.S. State Department: Guidelines for Application and Administration for Federal Assistance Awards Issued by the Department of State, available at http://fa.statebuy.state.gov/content/Documents/Recipient_Guidebook_Oct2011.pdf.

EXECUTIVE SUMMARY

The activities of USAID's PVS and the State Department's RAM are in direct conflict with European and UK data protection and privacy laws. Such laws do not permit either (i) the data processing necessary for the PVS and RAM or (ii) the transfer of personal data out of the European Economic Area[3] to the United States for the purposes of the PVS and RAM. Both hurdles — processing and transfer — must be satisfied in accordance with applicable law. While at first glance there may appear to be applicable exemptions to these requirements for the purposes of the PVS and RAM, a closer analysis of European and UK data protection and privacy law show this to not be the case (see below). We are hopeful that a solution to these hurdles can be found without the need for USAID and the State Department to engage in lengthy negotiations with the European Commission, as was necessary for the processing and transfer of passenger name records (see section IV.B below).

It bears emphasis that the data protection and privacy laws in the UK are relatively more pragmatic when compared to the laws in the rest of the European Union. Many other jurisdictions, such as France, have more stringent laws with further requirements, such as blocking statutes, violation of which carry criminal sentences.[4] Such blocking statutes are used to prevent cross-border data transfers for the purpose of compliance with foreign judicial or administrative proceedings.

Moreover, while the below addresses only EU and UK data protection and privacy laws, a number of other countries have adopted, or are in the process of adopting, similar EU-like data protection and privacy laws. Even within the pilot countries being proposed by the State Department and USAID, the Philippines and the Ukraine have passed data protection and privacy laws modelled on the EU laws, and we understand that privacy rights have been introduced into the new Kenyan constitution as well. While we do not directly address these laws below, we would note that the existence of these laws raises potentially serious questions about whether NGOs could comply with vetting and operate legally in these countries.[5]

For example, the Data Privacy Act of 2012 in the Philippines provides strict requirements, including mandatory data subject notification, conditions for lawful processing the provision of data subject rights, mandatory security requirements, and other requirements. Breach of the Data Privacy Act 2012 can result in severe sanctions including prisons sentences from three (3) to six (6) years and fines between PHP 500,000 and PHP 4,000,000 (approximately $12,000 USD to $96,000 USD).

3. The EEA includes the 28 EU Member States plus Norway, Lichtenstein and Iceland, all of which have enacted implementing legislation regarding these matters as if they were EU Member States.

4. See French Penal Law No. 80-538.

5. The following non-EU countries have adopted data protection laws that are similar to the Directive: Andorra, Argentina, Australia, Canada, Faroe Islands, Guernsey, Hong Kong, Iceland, Isle of Man, Israel, Jersey, Liechtenstein, Malaysia, Mexico, New Zealand, Norway, Peru, Philippines, Russia, Singapore, South Korea, Switzerland, Taiwan, Ukraine, United Arab Emirates (DFIC Zone) and Uruguay. Many more countries around the world also have data protection and privacy laws.

I. Territorial Scope of European Data Protection and Privacy Law

In the EU, data protection law and privacy law are two separate and distinct bodies of law. Data protection law governs the processing of personal data, being how individuals, companies, and public bodies can process and transfer personal data. These laws seek to ensure that personal data is processed or transferred only when certain conditions are met and that data subjects (being an identified or identifiable natural person whose personal data is processed) are provided with certain rights in respect of their personal data. In contrast, privacy law is about the fundamental right to respect for an individual's private and family life, his or her home, and his or her correspondence.

Below, we have discussed (A) the territorial scope of data protection law and (B) the territorial scope of privacy law.

A. Data Protection Law – Territorial Scope

In the EU, the Data Protection Directive (Directive 95/46/EC, the "**Directive**") governs the processing of personal data and the free movement of such data in the EU or in a place where its national law applies by virtue of public international law.[6] Note that if an individual never enters the EU but his or her personal data is still processed in the EU, as such expression is defined in the Directive, European data protection and privacy law can still apply.

The Directive imposes an obligation on EU Member States to enact a law substantially similar to the Directive into the national law of the Member State. The Member State transposition of the Directive must, at a minimum, provide the same protections and safeguards to personal data as found in the Directive. Unless Member State law is not properly *applying* the Directive in practice, the Directive does not have direct effect, meaning that an individual generally cannot directly rely on the Directive in court.[7]

In the UK, the Directive has been transposed into national law as the Data Protection Act 1998 (the "**DPA 1998**").[8] Both the Directive and the DPA 1998 have a limited territorial scope.

Under Article 4(a) of the Directive, the national law of a Member State shall apply where

> "processing is carried out in the context of the activities of an establishment of the controller *on the territory of the Member State*; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable" (*emphasis added*).[9]

---

6. *See* Directive 95/46/EC of the European Parliament and of the Council of October 24,1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.
7. *See* Case C-62/00 *Marks & Spencer plc v Commissioners of Customs & Excuse* [2002] ECR I-6325, [22] – [28].
8. *See* Data Protection Act 1998, available at http://www.legislation.gov.uk/ukpga/1998/29/contents.
9. A "'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his

Similarly, under Section 5(1)(a) of the DPA 1998, the DPA 1998 will apply only to a data controller that is "established in the United Kingdom and [when] the data are processed in the context of that establishment".

While establishment is not clearly defined under the Directive, Recital 19 explains that an establishment can be a branch office, subsidiary, or other entity where there is the "effective and real exercise of activity through stable arrangements". This means that where an NGO has an establishment in an EU Member State or where it is required to vet a European-based Partner, that Member State's law shall apply to the processing of personal data collected and/or processed by that establishment anywhere in the EEA.

If NGOs were to have no operations in the EEA, it is still possible to have European data protection law apply. Under Article 4(1)(c) of the Directive (and similarly under Section 5(1)(b) of the DPA 1998), national data protection law applies where a data controller is located outside the EEA but is processing personal data on equipment located inside the EEA for purposes other than mere transit (e.g., as a conduit or a connection wire) such that the data controller is exercising meaningful control over the equipment. Of course, US-based NGOs who partner with European institutions whose key personnel are in turn vetted by US-based NGOs would also implicate European data protection (as well as privacy) laws as personal data would be processed in Europe.

The definition of equipment is unclear and its interpretation is varied among the Member States. For example, in Spain, equipment means a database or server, while in the Netherlands, equipment can be an individual's computer or smart phone where a website uses those devices for processing by placing cookies or client-side java script on those devices. The European Commission interprets "equipment" as "means" so as to give equipment a very broad definition, such that any means used for processing will qualify as equipment, even cookies and client-side java script as is found in the Dutch interpretation of the law.[10]

The corollary of this is that where an NGO does not have operations in any Member State, and does not control equipment which processes personal data in any Member State, then that NGO may (from a location outside the EEA) collect personal data from within the European Union without infringing the Directive (although any organizations based in the EU that are involved in modifying or collecting that data from the EU would likely infringe the Directive).[11]

The difficulty with requiring US-based NGOs to collect data from Partners in the EEA (including European affiliates and sister organizations of US-based NGOs) in order to vet those Partners is that such requests will generally necessitate a formal request through those Partners' headquarters in the EEA. That information would then be collected through a human resources department or similar department of the EU Partner, before being transferred out of the EEA to the US-based NGO for the purpose of complying with the PVS or RAM. Therefore, the laws of the Member State in which the European Partner is located would apply to the personal data that is processed by that European Partner.

---

nomination may be designated by national or Community law", Article 2(d) of the Directive.

10. *See* Article 29 Working Party Opinion Paper on Applicable Law, WP 179, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf.

11. *Id.*

B. Privacy Law – Territorial Scope

On December 10, 1948, the United Nations General Assembly adopted the Universal Declaration of Human Rights ("**UDHR**") as a direct response to the atrocities that occurred during the Second World War.[12] Subsequently, in 1950, the newly formed Council of Europe drew on the inspiration of the UDHR in drafting the Convention for the Protection of Human Rights and Fundamental Freedoms or more commonly known as the European Convention on Human Rights ("**ECHR**").[13] Unlike the Directive, the ECHR is an international convention signed by 47 sovereign nations, including 20 nations outside the EU, and it imposes both positive and negative obligations on the state to not infringe an individual's human rights, as identified in the ECHR.

As the ECHR is an international convention, it requires its signatories to transpose the convention into its national law. In the UK, the ECHR was transposed into national law through the Human Rights Act 1998 ("**HRA 1998**").[14] Unlike a directive, the HRA 1998 functions by providing a recourse mechanism through which individuals can invoke the rights provided under the ECHR, first in the English courts and then in the European Court of Human Rights in Strasbourg but only where the English courts have failed to provide a remedy or where the English courts have found a piece of legislation incompatible with the ECHR and failed to provide a remedy.

Unlike the Directive, there is no qualification as to when the HRA 1998 applies. The HRA 1998 applies to all individuals and, in regard to privacy law, all information located in the United Kingdom. With respect to NGOs, the HRA 1998 applies to all information held in the European Union regardless of any other external factors.

II. Specific Requirements of European Data Protection Law which are in Conflict with PVS and RAM

It is a principle tenet of European data protection and privacy law that personal data may be processed only where certain conditions are met. Under the Directive, processing has a very wide definition and will cover the collection of personal data, the storing of personal data, making the personal data available to third parties, and the transfer of personal data from a country within the EEA to a country outside of the EEA.

For the purpose of the PVS and RAM, two circumstances are most important: (A) the actual right to process the data and (B) the right to transfer it outside the EEA.

A. Processing of Personal Data

Under the First Data Protection Principle of the DPA 1998, personal data must be processed fairly and lawfully, and, in particular, personal data may not be processed unless one of the conditions in Schedule 2 is met. With respect to NGOs subject to vetting under the PVS or RAM, schedule 2 of the

12. *See* The Universal Declaration of Human Rights, available at http://www.un.org/en/documents/udhr/.
13. *See* Convention for the Protection of Human Rights and Fundamental Freedoms, available at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=005&CM=8&DF=29/04/2013&CL=ENG.
14. *See* Human Rights Act 1998, available at http://www.legislation.gov.uk/ukpga/1998/42/contents.

DPA 1998 provides for the processing of personal data where:

1. The data subject has consented to the processing;
2. The processing is necessary for the performance of a contract to which the data subject is a party;
3. The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party to whom the personal data are disclosed;
4. The processing is necessary in the public interest; or
5. The processing is necessary for compliance with a legal obligation.

We will address each condition in turn below:

1. The Data Subject's Consent

The DPA 1998 does not provide a definition for the data subject's consent, but it is defined under the Directive as "any *freely given* specific and informed indication of [the data subject's] wishes by which the data subject signifies his agreement to personal data relating to him being processed" (*emphasis added*). Note that the mere fact that an individual has consented to the disclosure of his or her personal data on an NGO or Partner website, so as to make that personal data public, does not mean that the individual has consented to the processing of his or her personal data for the purposes of PVS or RAM. If USAID or the State Department were to vet the employee directly without involving the NGO, then the NGO would not be in breach of European data protection and privacy law.

The challenge with consent is that it must be freely given. This means that consent is valid only where there is no risk of deception, intimidation, coercion, or significant negative consequences where the data subject does not consent. Further, the EU Commission has expressed the opinion that consent in the employment relationship presents significant difficulty, as the employee may suffer adverse effects by declining consent.[15] Consequently, consent in the employment context is heavily scrutinized and is most likely not available as a viable solution in regard to employees.

For EU-based affiliates of the NGOs, providing such personal data on the employees of those affiliates would in all likelihood be within the context of employment. With respect to the consent of Partner organizations providing information for US-based NGOs, any such consent is clearly given on the condition that the US-based NGOs will receive the necessary funds. This consent as a prerequisite to receiving funds puts into question whether consent in these circumstances is freely given. In these circumstances, if the non-consent of the partners results in the US-based NGO or EU Partner not receiving the funds, then it is reasonable to argue that such non-consent resulted in significant negative consequences.

The EU Commission has provided a parallel example for passenger name record data, where it is stated that the choice between providing personal data and flying is not a real choice as the consequences (e.g., not being able to fly) of not consenting to supplying such personal data are too significant.[16] Similar to the employees, consent is not a viable solution for the Partners, as the consequences of

15. *See* Article 29 Working Party Opinion Paper on Consent, WP 187, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.
16. *Id*.

declining such consent are too significant.

Further, valid consent must be revocable, and where consent is revoked, it must be honored. In regard to US- or EU-based NGOs asking for the consent of their employees and the employees of their Partners, the NGOs submitting such data to USAID or the State Department will most likely not be able to honor the revocation of such consent once the personal data has been transferred to USAID or the State Department as USAID and the State Department will not cease processing the personal data for the PVS and RAM upon request and will not remove that data immediately upon the revocation of consent. It is arguable, therefore, that the consent obtained in such circumstances would be defective at law, and the NGOs should not seek to legitimize the processing of personal data of their employees or those of their partners for the PVS or RAM under the exemption of the data subject's consent.

2. Processing Necessary for the Performance of a Contract

On the assumption that both employees and Partners are under contract with the NGO submitting such data to USAID or the State Department and to the extent that such contracts require the processing of personal data for the PVS/RAM as a *necessity* to those contracts, such processing of personal data is lawful.

For this exemption to work, the key issue is the word "necessary". The UK data protection authority, the Information Commissioner's Office ("ICO"), explains that "necessary… imposes a strict requirement, because the condition will not be met if the organisation can achieve the purpose by some other reasonable means or *if the processing is necessary only because the organisation has decided to operate its business in a particular way*" (*emphasis added*).[17]

In regard to NGOs receiving funding from USAID or the State Department, the contracts for the employees and Partners might require NGOs to process the personal data of employees and Partners for the purposes of employing the employees and engaging the Partners, and in each case with the purpose of carrying out the functions of the NGOs (e.g., charity functions). This exception does not cover processing which is not necessary for those purposes and functions. In that respect, only a limited number of individuals would fall under this exception, namely those individuals who were hired for the express purpose of receiving and administering grants from USAID and the State Department.

Applying this to NGOs, would passing personal data to USAID or the State Department be necessary for the purpose of employing the employees and engaging the partners? Clearly, it is not necessary for NGOs to collect and pass to USAID or the State Department the personal data where the funds for those positions are obtained from a variety of sources, including nongovernmental sources (and this would be true for most employees). Therefore, the processing is not necessary in all cases, and in these cases — which would be for the majority of employees — the exception cannot be used.

For those employees who are employed solely to work on a USAID or State Department award, this exception might apply if the requirement that the individual's personal data must be submitted to the PVS or RAM database was made clear at the outset of employment. However, in reviewing the case, a court or regulator would also look at the applicability of other exceptions and see that compliance with

17. *See* ICO Guidelines: Conditions for Processing, available at http://ico.org.uk/for_organisations/data_protection/the_guide/conditions_for_processing.

a foreign legal obligation is not good grounds for the processing of personal data (see section II.A.5 below). There is a considerable risk that the court or regulator would take the view that the use of this exception in this way does not follow the spirit and purpose of the legislation and would therefore disallow it.

3. Legitimate Interests Exception

Similar to the contract exception above, a data controller can process personal data where the processing is "necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed".[18] The ICO provides that the "'legitimate interests' condition will not be met if the processing is unwarranted because of its prejudicial effect on the rights and freedoms, or legitimate interests, of the individual", and, in such cases, the individual has the additional right to object to the data processing.[19] This means that a balancing test must be conducted to examine whether there is a serious mismatch between the competing interests of the data subject and the data controller, and where there is such a mismatch, the data subject's legitimate interests will come first. This exception raises two concerns.

First, in regard to NGOs and the PVS and RAM systems, it is in the legitimate interest of the employees and Partners to not be exposed to physical harm.[20] This interest most likely far outweighs the interest of NGOs in sharing the personal data with USAID and the State Department. It would, however, need to be demonstrated that the employees and Partners are likely to face harm if their personal data is collected and shared with USAID or the State Department.[21]

Second, for the "rights and freedoms, or legitimate interests, of the individual" to be preserved, it is important that the individuals are able to exercise their rights under data protection law. In our view, it is also important that these rights are communicated to them as well. In order for the individual's rights to be preserved, USAID and the State Department would need to recognize European data protection law and afford the individual the same rights as if USAID and the State Department were directly subject to European data protection law.

These rights includes the right for all individuals (regardless of citizenship or residency) whose personal data is processed under European data protection and privacy law to have access to the personal data that USAID and the State Department holds about them; the right to correct erroneous personal data; the right to revoke consent; the right to prevent automatic processing of personal data; the right for

18. *Id*.

19. *Id.*; *see also* Article 14(a) of the Directive.

20. *See* Humanitarian Policy Group (HPG) Working Paper: Talking to the Other Side, Humanitarian engagement with the Taliban in Afghanistan, Ashley Jackson and Antonio Giustozzi, p. 13, December 2012 ("Aid agency sources mention a wave of abductions of NGO staff in 2010, apparently for intelligence-gathering purposes as the Taliban suspected NGOs of cooperating with their enemies").

21. We note that the significant press coverage regarding threats or killing of aid workers due to perceptions that they are affiliated with the US government intelligence agencies. For links to a small selection of these articles, *see*, *e.g.*, http://www.nytimes.com/2012/05/03/world/asia/bin-laden-raid-fallout-aid-groups-in-pakistan-are-suspect.html?pagewanted=all&_r=0; http://www.huffingtonpost.com/ali-hayat/shakil-afridi_b_1750005.html; http://www.huffingtonpost.com/ali-hayat/shakil-afridi_b_1750005.html; http://articles.latimes.com/2012/jan/15/world/la-fg-pakistan-ngos-20120115; http://www.nytimes.com/2011/11/29/world/asia/haqqani-militants-use-death-squads-in-afghanistan.html?_r=3&pagewanted=1&hp; http://www.reuters.com/article/2013/02/08/us-nigeria-violence-idUSBRE9170C120130208; http://www.forbes.com/sites/matthewherper/2013/02/08/more-polio-workers-killed/.

their personal data not to be used for any other purposes; and the right for personal data which is no longer necessary to be deleted. Although USAID the State Department and have designed the PVS and RAM to address the first two concerns to a certain extent,[22] USAID and the State Department have not agreed to afford European data subjects the full data protection rights required by European laws. Indeed, USAID stated in a rulemaking: "In any event, USAID is not inclined to ease or otherwise dilute its information requirements because European data protection authorities possibly might view PVS as a system that will not adequately protect information provided."[23] Without such protections, NGOs would be unable to comply with applicable data protection law; therefore, neither USAID, the State Department, nor the NGOs can make use of this exemption.

The European Commission will likely soon issue an opinion on the legitimate interests exception.[24] Similar opinions have been issued recently on other areas of data protection law, and, in such opinions, the European Commission has almost universally narrowed the scope of data processing permitted under applicable law.[25] While it cannot be predicted with certainty, we expect a similar narrowing of the legitimate interest exception in the forthcoming opinion.

4. Public Interest

Under the DPA 1998, personal data may be processed where it is necessary for reasons of substantial public interest. The ICO explains that there is a high threshold to meet in regard to what constitutes the public interest, and it is most likely to be relevant in areas such as "preventing or detecting crime".[26]

While it is reasonable to include the prevention of terrorism as a public interest, the ICO further explains that the public interest that is being served must be that of the UK and not a third country.

In regard to the PVS and RAM, the public interest can be defined as that of the US to not fund terrorism with US government funds. While the EU and the UK may share in the general public interest of combatting terrorism, the EU and the UK do not share in the public interest of how US government funds are spent. Moreover, the EU has repeatedly noted its concern in other situations with the US government's use of personal data for purposes of preventing terrorism, and the EU has made clear that stopping terrorist acts will not alone justify every use of personal data or the impingement upon the privacy rights of individuals located in the EU (*see* the cases in section III below). Consequently, we believe that NGOs cannot process personal data under the public interest exemption.

---

22. Privacy Act of 1974, Implementation of Exemptions, 74 Fed. Reg. 9, 12 (Jan. 2, 2009) (". . . all information submitted on individuals and maintained in the USAID system will be available for those individuals to request, review and correct."); Privacy Act; System of Records: State-78, Risk Analysis and Management Records, 76 Fed. Reg. 76,215, 76,217 (Dec. 6, 2011) ("Individuals who wish to gain access to or amend records pertaining to themselves should write to the Director, Office of Information Programs and Services . . . .").

23. Privacy Act of 1974, Implementation of Exemptions, 74 Fed. Reg. 9, 13 (Jan. 2, 2009).

24. See Article 29 Data Protection Working Party: Draft Agenda (main topics) for the 91st meeting June 5–6, 2013, available at http://ec.europa.eu/justice/data-protection/article-29/press-material/agenda/files/public_agenda_20130514_en.pdf.

25. *See* Article 29 Working Party Opinion Paper on Purpose Limitation, WP 203, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf; *see also* Article 29 Working Party Opinion Paper on Consent, WP 187, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.

26. *See* ICO Guidelines: Conditions for Processing, available at http://ico.org.uk/for_organisations/data_protection/the_guide/conditions_for_processing.

5. Legal Obligation

Lastly, personal data may be processed in furtherance of a legal obligation (not including obligations imposed by contract). But, similar to the public interest exception, the legal obligation must be that of a UK legal obligation or an EU legal obligation.[27] To that end, some consideration is given for foreign legal obligations that are mirrored in English law or EU law, but where a legal obligation exists entirely outside the realm of English or EU law, the exemption is not available. In regard to the PVS or RAM, no such program exists under English law or EU law which presents a direct legal obligation on NGOs, and, consequently, this legal obligation exception is not available to NGOs for the PVS or RAM. The UK Foreign & Commonwealth Office has, however, requested similar vetting information from NGOs through contract in its Accountable Grant Agreement, subject to the boundaries of the DPA 1998.[28]

B. Data Transfer outside the European Economic Area

Under the DPA 1998's 8th data protection principle, personal data may not be transferred out of the EEA unless "the [destination] country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data". An "adequacy" decision is made by the European Commission, and at present does not include the United States except where a company self certifies with the U.S. Safe Harbor program — a program which allows a U.S. company to self-adhere to a set of principles that are somewhat analogous to European data protection and privacy law, thereby receiving an adequacy finding via the Safe Harbor Program.[29] The Safe Harbor Program is not available to governmental organizations.

Where the destination does not have an adequacy decision, Schedule 4 of the DPA 1998 provides a lists of exemptions under which a personal data transfer may be made. In regard to NGOs transferring personal data under the DPA 1998 to USAID or the State Department, the available exemptions are:

1. The data subject has given his or her consent to the transfer;
2. Where the transfer is necessary for reasons of substantial public interest; or
3. Where the transfer is made on terms which are of a kind approved by the ICO, as ensuring adequate safeguards for the rights and freedoms of data subjects (e.g., data transfer agreement).

There is also an additional exemption under the DPA 1998 from the non-disclosure requirement:

4. Where the disclosure is required by or under any enactment, by any rule of law, or by the order of a court.

We will address each condition in turn below, but please note that both a condition for processing as described above and an exemption for data transfer must be met in order to comply with data protection law.

---

27. *Id. See also* Article 29 Working Party Opinion Paper on a Common Interpretation of Article 26(1) of Directive 95/46/EC, WP 114, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf.
28. *See* Foreign & Commonwealth Office: Accountable Grant Agreement, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192447/Accountable_Grant_Agreement.pdf.
29. *See* Commission decisions on the adequacy of the protection of personal data in third countries, available at http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm#h2-12.

1. The Data Subject's Consent

The same analysis that was used above under data processing consent applies here, where the consent is for the transfer of personal data outside the EEA. Consequently, the data subject's consent is not a valid method to legitimize the transfer of personal data.

2. Substantial Public Interests

Generally, the same analysis that was used above under data processing in the public interest applies here to the transfer of personal data outside the EEA. However, there is a difference in that the public interest exception to data transfers does consider where the international exchange of data might be necessary. The European Commission specifically makes mention of data transfers "between tax or customs administrations in different countries" or "between services competent for social security matters".[30] The European Commission then states that this exception may be used only if the transfer is of interest to the authorities of an EU Member State themselves, and not only to one or more public authorities in the third country.[31]

In regard to the transfer of data to USAID and the State Department, the transfer is not between two public authorities but between the NGOs and U.S. public authorities, as the transfer is not of interest to a specific European government. Consequently, it is not possible for the NGOs to legitimize the data transfer pursuant to the public interests of the United States.

3. Data Transfer Agreement

It is permissible to transfer personal data to a data importer in a country without an adequate level of data protection and privacy law where that data importer has agreed through contract to adhere to obligations substantially similar to those obligations found under the DPA 1998.[32] While it is possible for European-based affiliates or offices of NGOs or European-based Partners to enter into a data transfer agreement with their U.S. NGO counterparts, it will not be possible for the NGOs in the U.S. to onward transfer the personal data to USAID or the State Department. This is because we believe it is unlikely that USAID or the State Department would enter into EU Model Contractual Clauses with US-based NGOs due to the requirements on the data importer to provide data processing safeguards and assistance with honoring data subject access requests. For example, the PVS and RAM do not allow data subjects to appeal any positive "match" of their data against an individual in the government databases; the systems do not allow those data to be corrected once the data are in the systems; and there are not other forms of clear remediation in regard to any false positives or the general maintenance of the personal data held in the PVS or RAM.

4. Disclosures Required by or under Any Enactment, by Any Rule of Law, or by the Order of a Court

Under Section 35 of the Act, an exemption is provided for disclosures required by or under any

30. *See* Article 29 Working Party Opinion Paper on a Common Interpretation of Article 26(1) of Directive 95/46/EC, WP 114, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf.

31. *Id.*

32. *See* EU Model Contractual Clauses, available at http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm.

enactment, by any rule of law, or by the order of a court. It is important to note here that this exemption is not an exemption to the 8th data protection principle but only to the non-disclosure requirements of the 1st, 2nd, 3rd, 4th and 5th data protection principles and Sections 10 and 14 of the DPA 1998.

This means that any disclosure in furtherance of a legal obligation must be that of an EU legal obligation. This point is further made by the ICO in its guidance on the 8th data protection principle and by the European Commission in its opinion paper on international data transfers out of the EEA.[33] Consequently, a U.S. legal obligation is not a sufficient exemption to transfer personal data from the EU to the U.S. However, the ICO does recommend that they be consulted on such transfers, and, where appropriate, the ICO can grant permission to transfer personal data in furtherance of a foreign legal obligation.[34]

III. Specific Requirements of European Privacy Law which are in Conflict with the PVS and RAM

As discussed above, the HRA 1998 seeks to protect the fundamental human rights of all individuals in the UK through the provisions of the ECHR. This specifically includes the right to respect for an individual's private and family life, his or her home, and his or her correspondence.[35] The right to a private life is a broad right and includes the right to the preservation of one's physical integrity.[36] Further, the right to a private life includes the protection of personal data where the collection, use, and disclosure of such personal data infringes such right.[37] In regard to the PVS and RAM, it can be argued that the collection, processing, and disclosure of personal data of employees and Partners interferes with their right to a private life where such processing exposes employees and Partners to physical harm.

However, the right to privacy is a qualified right, and, therefore, interference with this right is permissible where "[the interference] is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".[38] The question then becomes to what extent can a government's justifications to interfere with ECHR privacy rights be in accordance with the law?

In *Kennedy v. the United Kingdom*, it was held that any interference with an individual's privacy right is possible only where three conditions are met — the first condition being that there must be some basis in domestic law.[39] As the PVS and RAM are offered through USAID and the State Department

33. *Id*. *See also* Article 29 Working Party Opinion Paper on a Common Interpretation of Article 26(1) of Directive 95/46/EC, WP 114, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf.

34. *See* ICO guide to Sending personal data outside the European Economic Area (Principle 8), available at http://ico.org.uk/for_organisations/data_protection/the_guide/principle_8.

35. *See* Article 8, The European Convention of Human Rights, available at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=005&CM=8&DF=29/04/2013&CL=ENG.

36. *See X and Y v the Netherlands* [1985] ECHR 4.

37. *See MS v Sweden* (1999) 28 EHRR 313.

38. *See* Article 8(2), The European Convention of Human Rights, available at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=005&CM=8&DF=29/04/2013&CL=ENG.

39. *See Kennedy v. the United Kingdom*, no. 26839/05, 18.8.2010, explaining that any interference should be 'in accordance

and not through the UK or another Member State or even with the participation and cooperation of the UK or another Member State, there is no basis in EU or Member State law for either program.

Thus, where USAID and the State Department seek to process employee and Partner personal data at the cost of the employees' and Partners' right to a private life, the PVS and RAM are in direct conflict with the ECHR.

IV. Examples of Conflict of Laws in Relation to European Data Protection and Privacy Law

Where the DPA 1998 and ECHR (via the HRA 1998) apply and do not permit compliance with the PVS or RAM as discussed above, there is a conflict of laws. Historically, action has been taken on a case-by-case basis, and the four most notable cases are that of (i) the Society for Worldwide Interbank Financial Telecommunication ("**SWIFT**"); (ii) U.S. Passenger Names Record Data; (iii) UBS Client Data; and (iv) the French case of *In re Advocat "Christopher X"* ("**Christopher X**").

A. Society for Worldwide Interbank Financial Telecommunication

Under U.S. law, SWIFT was to provide personal data to the U.S. Treasury's Office of Foreign Assets Control ("**OFAC**") on the basis of the Terrorist Finance Tracking Program ("**TFTP**").[40] OFAC reasoned that information derived from the use of SWIFT personal data aided the U.S. and foreign nations to better identify the financiers of terrorism, but this justification alone was considered insufficient to legitimize the transfer of SWIFT personal data to the U.S.[41] Ultimately, the EU and the U.S. entered into an agreement to specifically regulate the transfer of SWIFT personal data to OFAC after a long and extensive period of negotiations and published government opinions, thereby resolving the conflict between the conflicting legal obligations of the EU and U.S.[42]

---

with the law' under art 8(2) would only be met where three conditions were satisfied. First, the impugned measure should have some basis in domestic law. Second, the domestic law should be compatible with the rule of law and accessible to the person concerned. Third, the person affected should be able to foresee the consequences of the domestic law for him; *see also Weber and Saravia v. Germany*, no. 54934/00, June 29, 2006.

40. *See* Europa Press Release: The SWIFT case and the American Terrorist Finance Tracking Program, 28/06/2007, available at http://europa.eu/rapid/press-release_MEMO-07-266_en.htm?locale=EN.

41. Belgian Data Protection Commission, 'Opinion No. 37/2006 of 27 September 2006 on the transfer of personal data by the CSLR SWIFT by virtue of UST (OFAC) subpoenas'; *see also* Article 29 Working Party Opinion Paper on Society for Worldwide Interbank Financial Telecommunication (SWIFT), WP 128, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf.

42. *See* Article 29 Working Party Opinion on transmission of Passenger Manifest Information and other data from Airlines to the United States, WP 66, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp66_en.pdf; *See also* Article 29 Working Party Opinion on the Level of Protection ensured in the United States for the Transfer of Passengers' Data, WP 78, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/2003-06-23-prn-apis_en.pdf; Article 29 Working Party Opinion on the implementation of the Commission decision of 14-V-2004 on the adequate protection of personal data contained in the Passenger Name Records of air passengers transferred to the United States' Bureau of Customs and Border Protection, and of the Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, WP 95, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp95_en.pdf; Article 29 Working Party Opinion on the information for passengers concerning the transfer of PNR data on flights between the European Union and the United States of America, WP 97, available at http://

B. Passenger Name Records Data

Under U.S. law, the U.S. Customs and Border Protection ("**CBP**") wanted to receive certain travel and reservation personal data (PNR data) about passengers traveling from the EU to the U.S.[43] Without an adequacy decision or other safeguards, this transfer of personal data was considered to be unlawful under European data protection and privacy law.[44] Ultimately, the EU and the U.S. entered into an agreement legitimizing the specific transfer of PNR data from the EU to the Department of Homeland Security, CBP's parent organization, in the U.S.[45]

C. UBS Client Data

In 2009, the United States Internal Revenue Service ("IRS") was investigating UBS AG ("**UBS**") in regard to American tax dodgers.[46] As part of this investigation, the IRS asked a U.S. district court to order UBS to disclose the identities of U.S. clients with secret Swiss bank accounts. Initially, the Swiss government refused the subpoena and argued that the subpoena violated Swiss data protection and privacy law. Ultimately, the United States and Switzerland entered into an agreement to regulate the transfer of personal data from Switzerland to the United States for the purpose of the subpoena.[47]

---

ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp97_en.pdf; Article 29 Working Party Opinion on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States, WP 122, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp122_en.pdf; Article 29 Working Party Opinion on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States and the urgent need for a new agreement, WP 124, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp124_en.pdf; Article 29 Working Party Opinion on information to passengers about transfer of PNR data to US authorities, WP 132, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp132_en.pdf; Article 29 Working Party Opinion on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007, WP 138, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp138_en.pdf; Article 29 Working Party Opinion on information to passengers about the transfer of PNR data to US authorities, Adopted on February 15, 2007 and revised and updated on June 24, 2008, WP 151, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp151_en.pdf.

43. *See* Article 29 Working Party Opinion Paper on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP), WP 87, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp87_en.pdf.

44. *Id*.

45. *See* AGREEMENT between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/l_204/l_20420070804en00180025.pdf; *see also* COUNCIL DECISION 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement).

46. *See* market Watch: IRS tries to force UBS to reveal U.S. tax dodgers, available at http://articles.marketwatch.com/2009-02-19/news/30798166_1_account-holders-secret-swiss-bank-accounts-ubs-ag.

47. *See* Agreement between the United States of America and the Swiss Federation on the request for information from the Internal Revenue Service of the United States of America regarding UBS AG, a corporation established under the laws of the Swiss Confederation, available at http://www.irs.gov/pub/irs-drop/us-swiss_government_agreement.pdf.

D. Christopher X

In 2008, the French Supreme Court upheld the criminal conviction of a French lawyer for violating the French blocking statute by complying with a request from a U.S. court; the convicted lawyer was fined 10,000 Euros but did not receive a prison sentence (potentially up to six months).[48] The French blocking statute requires:

> "Subject to international treaties or agreements and laws and regulations in force, it is forbidden for any person to request, seek or communicate in writing, orally or in any other form, documents or information of an economic, commercial, industrial, financial nature leading to the constitution of evidence with a view to foreign judicial or administrative procedures or in the context of such procedures."[49]

This decision confirmed that parties caught in France communicating information relating to economic, commercial, or financial matters may be prosecuted under the French blocking statute and that international conventions are the exclusive means of securing information in France for use in foreign matters.

Based on these precedents, we believe that NGOs who are collecting or forwarding the personal data of their European affiliates, offices, or Partners for purposes of complying with the PVS or RAM would face significant risks with respect to violations of EU data protection and privacy laws.

V. Police and Judicial Co-operation in Criminal Matters

In 2003, the EU and the United States entered into a Mutual Legal Assistance Agreement ("**MLAA**") to facilitate collaboration for the purposes of criminal investigations and counter-terrorist activities.[50] The MLAA provides specific circumstances and on what conditions the EU and the United States may exchange information under the MLAA. It is possible for the EU or a Member State to enter into such an agreement because the Directive and its national implementations do not apply to Member State data processing concerning public security, defence, Member State security, and the activities of the Member States in areas of criminal law.[51]

The exchange of information under the MLAA must be between the Contracting Parties – the EU and the U.S.[52] With respect to the PVS and RAM, there is no evidence that the United States has sought the cooperation of the European Union or any Member States to obtain the necessary information from the required NGOs. Without such cooperation, the United States may not rely upon the MLAA to resolve the conflict of law between the PVS and RAM and European data protection and privacy law.

---

48. *See* Cour de cassation [Cass.] [supreme court for judicial matters] Paris, crim., Dec. 12, 2007, Bull. crim., No. 7168 [JurisData No. 2007-83228] (Fr.).
49. *See* French Penal Law No. 80-538.
50. *See* Agreement on the mutual legal assistance between the European Union and the United States of America, OJ L 181/34, July 19, 2003, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:181:0034:0042:en:PDF.
51. *See* Article 3(2) of the Directive.
52. *Id* at Article 1.

If the EU were to cooperate with the United States in respect of the PVS and RAM, such cooperation must comply with Article 9 of the MLAA (limitations on use to protect personal data and other data). Article 9 states that the requesting State may use any evidence or information obtained from the requested State for the purpose of criminal investigations and proceedings and for preventing an immediate and serious threat to public security, as well as other limited purposes. If the evidence or information is to be used for a purpose which is not covered by Article 9, the requesting State must obtain the consent of the requested State.

As the PVS and RAM do not address any particular investigation nor do they seek to remedy an immediate or serious threat, it is difficult to argue that the PVS and RAM are permissible under Article 9 without specific consent from the European Union or the participating Member State.

If, however, the United States were to make a request under the MLAA to a Member State, the Member State may provide personal data to the United States only in accordance with Council Framework Decision 2008/977/JHA (the "**Framework Decision**").[53] Similar to the Directive, the Framework Decision regulates the processing and transfer of personal data. However, the Framework Decision applies to Member States for the purpose of police and judicial cooperation in the prevention, investigation, detection, or prosecution of a criminal offense or execution of a criminal penalty.

Additional mechanisms under which the European Union may exchange information with the United States also exist, such as Europol[54] and Eurojust.[55] These have not been discussed in this article as there is yet to be any evidence of USAID or the State Department involving European authorities with the PVS and RAM.

VI. Penalties and Sanctions for Violations of the DPA 1998

Although the fines for violations of EU Member State laws may vary from country to country, breaches of obligations imposed under the DPA 1998 may result in (i) compulsory audits; (ii) financial sanctions of up to £500,000 GBP; and/or (iii) criminal fines of up to £5,000 GBP per breach of the DPA 1998.[56] At present, only monetary penalties are imposed on those individuals who are found culpable under the DPA 1998. NGOs that have offices or are working with Partners in more than one EU country could face fines from multiple countries.

Further, an individual who has had his or her rights violated by a data controller may seek both monetary compensation and injunctive relief in court.[57] However, there has been little success for data

53. *See* Council Framework Decision 2008/977/JHA of November 27, 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30/12/2008, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:01:EN:HTML.

54. Council Decision 2009/371/JHA establishing the European Police Office, OJ L121/37, available at https://www.europol.europa.eu/sites/default/files/council_decision.pdf.

55. *See* Council Decision 2002/187/JHA of February 28, 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 63/1, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:063:0001:0013:EN:PDF.

56. *See* Sections 21, 40, 41, 55 and 60 of the Act.

57. *See* Sections 13 and 15 of the Act.

subjects in court due to the difficulty in proving quantifiable damage and distress.[58]

Lastly, within the next few years, a new regulation, the General Data Protection Regulation ("**GDPR**"), is expected to come into force and replace the Directive.[59] Under Article 79 of the GDPR, sanctions can reach up to 1,000,000 Euros for a data controller who intentionally or negligently breaches the GDPR.

CONCLUSION

Any processing of personal data for the purposes of the PVS and RAM presents an inherent conflict with European data protection and privacy law. Without an agreement or other mechanism in place between the EU and the United States, NGOs required to process and transfer personal data for the purposes of the PVS and RAM are forced to choose between breaching European data protection and privacy law and forgoing USAID and State Department grants or other assistance.

If USAID and the State Department wish to continue the PVS and RAM, USAID and the State Department should seek to mitigate those aspects of the PVS and RAM which most conflict with European data protection and privacy law, as well as make use of the diplomatic channels designed to remedy circumstances such as those which result in a conflict of law (see section III above). Until then, NGOs subject to European data protection and privacy law will continue to lack the necessary legal basis to lawfully process and transfer the personal data of their key employees and Partners to the United States for the purposes of the PVS and RAM.

58. ICO Complaints, available at http://www.ico.gov.uk/complaints/data_protection.aspx. The UK government has undergone consultations on the topic of introducing a prison sentence in some instances.

59. *See* Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

About

The Project on Counterterrorism and Humanitarian Engagement (CHE Project) is based at the Harvard Law School. The CHE Project undertakes legal research, policy analysis, and engagement initiatives in order to identify and develop — as well as to facilitate networks to support — sustainable, principled, and practical solutions to the challenges of large-scale humanitarian operations conducted in areas where listed armed groups are active and counterterrorism laws affect humanitarian action.

This publication is part of the CHE Project's Research and Policy Paper series, which is intended to inform the humanitarian community regarding critical issues of law, policy, and practice related to counterterrorism and humanitarian action.

The CHE Project seeks to inform and shape debate regarding the intersecting trajectories of counterterrorism norms and humanitarian action. The Project does so principally by:

- Producing independent analyses of emerging and foundational challenges and opportunities concerning humanitarian engagement in situations involving listed non-state armed actors; and

- Engaging actors across international humanitarian NGOs, intergovernmental agencies, academic centers, and governments to capture, examine, and inform their perspectives and approaches.

The Counterterrorism and Humanitarian Engagement Project receives generous support from the Swiss Federal Department of Foreign Affairs.

Contact

Naz K. Modirzadeh
Senior Fellow
HLS-Brookings Project on Law and Security
Counterterrorism and Humanitarian Engagement Project
Harvard Law School
nmodirzadeh@law.harvard.edu