THE EU DIRECTIVE ON DATA PROTECTION AND THE US "SAFE HARBOR"

HINCKLEY ALLEN

Providing Value.
Delivering Results.

This white paper is intended for general information purposes only. It is not intended as legal advice. The reader is urged to consult a qualified advisor before making any decisions relating to the matters discussed in this white paper.

AUTHORED BY:
Mark Hichar
Partner, Gaming and Co-Chair, International

November 2014

The EU Directive

The European Commission's Directive on Data Protection (the "Directive")[1] was enacted in 1995 and went into effect in 1998. It would prohibit the transfer of personal data from European Union ("EU") countries to non-European countries that do not meet the EU "adequacy" standard for privacy protection.

SCOPE OF THE DIRECTIVE

The Directive applies to the **"processing"** of **"personal data."**

> "Personal data" is defined as "any information relating to an identified or identifiable natural person," where "an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."
>
> "Processing of personal data" is defined as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, . . . retrieval, . . . use, disclosure by transmission, dissemination or otherwise making available, . . ."

The Directive applies to **"controllers"** of personal data.

> A "controller" is defined as "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 . . ."

The Directive does not apply to the processing of personal data:

- for purposes concerning public security, national defense, national security . . . and the activities of a nation in areas of criminal law, or
- by a natural person in the course of a purely personal or household activity.

In addition, EU member states may adopt laws to restrict the application of the law when it deems such a restriction is necessary to safeguard:

- national security;
- national defense;
- public security;
- the prevention, investigation, detection, and prosecution of criminal offences, or of breaches of ethics for regulated professions; or
- the protection of the data subject or of the rights and freedoms of others.

[1] The EU's Data Protection Directive is more formally known as Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It can be found in its entirety at the EU Data Protection Commissioner's website at http://www.dataprotection.ie/docs/EU-Directive-95-46-EC/89.htm.

The "Safe Harbor" framework

provides a streamlined and cost-effective means for US organizations to satisfy the Directive's "adequacy" requirement, thereby avoiding interruptions in their business dealings with the EU or becoming subject to prosecution by EU member state authorities under EU member state privacy laws.

A CONTROLLER'S OBLIGATIONS UNDER THE DIRECTIVE

The Controller must ensure that personal data is (among other things):

- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. (Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided appropriate safeguards are in place);
- not excessive in relation to the purposes for which it is collected and/or further processed;
- accurate and, where necessary, kept up to date (every reasonable step must be taken to ensure that data which is inaccurate or incomplete is erased or corrected);
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed.

In addition, personal data may be processed only if:

- the data subject has unambiguously given his/her consent;
- processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at his/her request prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject; or
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed.

TRANSMISSION OF PERSONAL DATA OUTSIDE THE EU ALLOWED ONLY IF "ADEQUATELY" PROTECTED

EU member states must provide in their laws that the transfer of personal data to countries outside the EU for processing may occur only if the non-EU country in question ensures in its laws an "adequate" level of protection for personal data.

The US "Safe Harbor"[2]

In order to provide a streamlined means for US organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed a "Safe Harbor" framework deemed to "adequately" protect personal data[3] and thus be compliant with the Directive. It was approved by the EU in 2000.

RATIONALE

The Directive would prohibit the transfer of personal data to non-EU countries that do not meet the EU's "adequacy" standard for protecting the confidentiality of such personal data. The lack of straightforward measures that clearly complied with the Directive could have severely restricted the ability of US organizations to engage in a variety of trans-Atlantic transactions.

The "Safe Harbor" framework provides a streamlined and cost-effective means for US organizations to satisfy the Directive's "adequacy" requirement, thereby avoiding interruptions in their business dealings with the EU or becoming subject to prosecution by EU member state authorities under EU member state privacy laws.

Self-certifying to the US-EU Safe Harbor framework gives assurance to EU organizations that your organization provides "adequate" privacy protection with respect to personal data, as defined by the Directive.

BENEFITS OF UTILIZING THE SAFE HARBOR

All 28 member states of the EU will be bound by the European Commission's finding of "adequacy."

Participating US organizations will be deemed to provide "adequate" privacy protection, within the meaning of the Directive.

An EU organization can be sure that it is sending information to a US organization participating in the US-EU Safe Harbor program by viewing the public list of Safe Harbor organizations posted at the U.S. International Trade Association's website.[4]

Member State requirements for prior approval of data transfers will be waived, or approval will be automatically granted.

Claims brought by EU citizens against US organizations will be heard in the United States, subject to limited exceptions.

Compliance requirements are streamlined and cost-effective – a particular benefit to small- and medium-sized enterprises.

[2] Much of this information describing the Safe Harbor is taken from the U.S. International Trade Administration's ("ITA") website at: http://export.gov/safeharbor/ and http://export.gov/safeharbor/eu/eg_main_018475.asp. (The ITA is an agency within the U.S. Department of Commerce.)

[3] For purposes of the Safe Harbor, "personal data" and "personal information" are data about an identified or identifiable individual that are within the scope of the Directive, received by a US organization from the European Union, and recorded in any form.

[4] The ITA's website at which the public list may be viewed is at http://safeharbor.export.gov/list.aspx.

HOW TO OBTAIN THE BENEFITS OF THE SAFE HARBOR

Entering the Safe Harbor program is voluntary. To enter, an organization must:

- comply with the Safe Harbor "Privacy Principles";
- publicly declare that it complies with the Safe Harbor, including in its published privacy policy; and
- self-certify annually to the U.S. Department of Commerce in writing that it adheres to the Safe Harbor requirements.

To qualify for the Safe Harbor, an organization can either (1) join a self-regulatory privacy program that adheres to the Safe Harbor requirements; or (2) develop its own self-regulatory privacy policy that conforms to the Safe Harbor framework.[5]

ELIGIBILITY FOR SELF-CERTIFICATION

Only US organizations subject to the jurisdiction of the Federal Trade Commission ("FTC"), or US air carriers and ticket agents subject to the jurisdiction of the Department of Transportation, may participate in the Safe Harbor. In general, organizations not subject to FTC jurisdiction include certain financial institutions (such as banks, investment houses, credit unions, and savings & loan institutions), telecommunication common carriers, labor associations, non-profit organizations, agricultural co-operatives, and meat processing facilities. In addition, the FTC's jurisdiction with regard to insurance activities is limited to certain circumstances. (In cases of uncertainty, contact those agencies and/or your counsel.)

THE SAFE HARBOR PRIVACY PRINCIPLES AND WHAT THEY REQUIRE

1 Notice

An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal data to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.[6]

2 Choice

An organization must offer individuals the opportunity to choose (opt out) whether their personal data is (a) to be disclosed to a third party[7] or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

---

[5] When an organization relies in whole or in part on self-regulation, its failure to comply with such self-regulation must also be actionable under the Federal Trade Commission Act or other law prohibiting unfair and deceptive acts or another law or regulation prohibiting such acts, else the organization is not eligible to join the Safe Harbor.

[6] It is not necessary to provide notice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The "Onward Transfer" Principle, on the other hand, does apply to such disclosures.

[7] See footnote 6.

For sensitive information (i.e., personal data specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership or information specifying the sex life of the individual), individuals must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt-in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.

3 Onward Transfer

To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as the organization's agent,[8] it may do so if it first ascertains that (i) the third party agent subscribes to the Safe Harbor Principles, (ii) the third party agent is subject to the Directive or another adequacy finding, or (iii) the organization enters into a written agreement with such third party agent requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known that the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.

4 Security

Organizations creating, maintaining, using or disseminating personal data must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

5 Data Integrity

Consistent with the Safe Harbor Privacy Principles, personal data must be relevant for the purposes for which it is to be used. An organization may not process personal data in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

6 Access

Individuals must have access to personal data about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

7 Enforcement

Effective privacy protection must include mechanisms for ensuring compliance with the Safe Harbor Privacy Principles, recourse for individuals to whom the data relate and who are affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum,

[8] See footnotes 5 and 6.

such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and by which damages are awarded where the applicable law or private sector initiatives so provide; (b) follow-up procedures for verifying that the representations businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them, and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles will apply on a regular basis.

EXCEPTIONS TO THE REQUIREMENTS OF THE SAFE HARBOR PRIVACY PRINCIPLES

Similar to the Directive, adherence to the Safe Harbor Privacy Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive or EU member state law is to allow exceptions or exemptions, provided such exceptions or exemptions are applied in comparable contexts.

Organizations may wish for practical or other reasons to apply the Principles to all their data processing operations, but they are obligated only to apply them to data transferred after they enter the Safe Harbor.

To qualify for the Safe Harbor, organizations are not obligated to apply the Safe Harbor Privacy Principles to personal data in manually processed filing systems. However, organizations wishing to benefit from the Safe Harbor for receiving information in manually processed filing systems from the EU must apply the Principles to any such information transferred after they enter the Safe Harbor.

An organization that wishes to extend Safe Harbor benefits to human resources personal data transferred from the EU for use in the context of an employment relationship must indicate this when it self-certifies to the Department of Commerce (or its designee) and conform to all Safe Harbor requirements set forth in the Frequently Asked Question on Self-Certification. (See **Exhibit 1**.)

US LAW APPLIES

US law will apply to questions of interpretation and compliance with the Safe Harbor Principles and other relevant provisions related to the Safe Harbor framework, except where organizations have committed to cooperate with European data protection authorities.

ENFORCEMENT

In general, enforcement of the Safe Harbor will take place in the United States in accordance with US law and will be carried out primarily by the private sector – self-regulation. (However, see **Exhibit 1** regarding human resources information.) Private sector self-regulation and enforcement will be backed up as needed by government enforcement of the federal and state "unfair and deceptive" statutes.

Private Sector Enforcement

As part of their Safe Harbor program obligations, organizations are required to have in place a dispute resolution system that will investigate and resolve individual complaints and disputes and to have procedures for verifying compliance. They are also required to remedy problems arising out of a failure to comply with the principles. Sanctions that dispute resolution bodies can apply must be severe enough to ensure compliance by the organization; they must include publicity for findings of non-compliance and deletion of data in certain circumstances. They may also include suspension from membership in a privacy program (and thus effectively suspension from the US-EU Safe Harbor program) and injunctive orders.

Government Enforcement

Depending on the industry sector, the FTC, comparable US government agencies, and/or the states may provide overarching government enforcement of the Safe Harbor Privacy Principles. Where an organization relies in whole or in part on self-regulation in complying with the Safe Harbor Privacy Principles, its failure to comply with such self-regulation must be actionable under federal or state law prohibiting unfair and deceptive acts, else it is not eligible to join the Safe Harbor.

Under the Federal Trade Commission Act,[9] for example, an organization's failure to abide by commitments to implement the Safe Harbor Privacy Principles might be considered deceptive and actionable by the FTC. This is the case even where an organization adhering to the Safe Harbor Privacy Principles relies entirely on self-regulation to provide the enforcement required by the Safe Harbor enforcement principle. The FTC has the power to rectify such misrepresentations by seeking administrative orders and civil penalties of up to $16,000 per day for violations.

If an organization persistently fails to comply with the US-EU Safe Harbor framework requirements, it is no longer entitled to benefit from the US-EU Safe Harbor. Persistent failure to comply arises where an organization refuses to comply with a final determination by any self-regulatory or government body or where such a body determines that an organization frequently fails to comply with the requirements to the point where its claim to comply is no longer credible. In these cases, the organization must promptly notify the Department of Commerce of such facts. Failure to do so may be actionable as a crime under the False Statements Act.[10]

The Department of Commerce's public list of organizations self-certifying adherence to the US-EU Safe Harbor framework requirements will indicate any notification it receives of persistent failure to comply and will make clear which organizations are assured and which organizations are no longer assured of the Safe Harbor benefits.

[9] 15 U.S.C. § 41 et seq.

[10] 18 U.S.C. § 1001.

EXHIBIT 1: FAQS REGARDING THE APPLICATION OF SAFE HARBOR BENEFITS TO HUMAN RESOURCES PERSONAL DATA [11]

Question 1 **Is the transfer from the EU to the United States of personal information collected in the context of the employment relationship covered by the Safe Harbor?**

Yes, where a company in the EU transfers personal information about its employees (past or present) collected in the context of the employment relationship, to a parent, affiliate, or unaffiliated service provider in the United States participating in the Safe Harbor, the transfer enjoys the benefits of the Safe Harbor. In such cases, the collection of the information and its processing prior to transfer will have been subject to the national laws of the EU country where it was collected, and any conditions for or restrictions on its transfer according to those laws will have to be respected.

The Safe Harbor Principles are relevant only when individually identified records are transferred or accessed. Statistical reporting relying on aggregate employment data and/or the use of anonymized or pseudonymized data does not raise privacy concerns.

Question 2 **How do the Notice and Choice Principles apply to such information?**

A US organization that has received employee information from the EU under the Safe Harbor may disclose it to third parties and/or use it for different purposes only in accordance with the Notice and Choice Principles. For example, where an organization intends to use personal information collected through the employment relationship for non-employment-related purposes, such as marketing communications, the US organization must provide the affected individuals with choice before doing so, unless they have already authorized the use of the information for such purposes. Moreover, such choices must not be used to restrict employment opportunities or take any punitive action against such employees.

It should be noted that certain generally applicable conditions for transfer from some Member States may preclude other uses of such information even after transfer outside the EU and such conditions will have to be respected.

In addition, employers should make reasonable efforts to accommodate employee privacy preferences. This could include, for example, restricting access to the data, anonymizing certain data, or assigning codes or pseudonyms when the actual names are not required for the management purpose at hand.

To the extent and for the period necessary to avoid prejudicing the legitimate interests of the organization in making promotions, appointments, or other similar employment decisions, an organization does not need to offer notice and choice.

Question 3 **How does the Access Principle apply?**

The FAQs on access provide guidance on reasons which may justify denying or limiting access on request in the human resources context. Of course, employers in the EU must comply with local regulations and ensure that EU employees have access to such information as is required by law in their home countries, regardless of the location of data processing and storage. The Safe Harbor requires that an organization processing such data in the United States will cooperate in providing such access either directly or through the EU employer.

[11] This information is taken from the U.S. International Trade Administration's website at http://export.gov/safeharbor/eu/eg_main_018381.asp.

Question 4 **How will enforcement be handled for employee data under the Safe Harbor Principles?**

In so far as information is used only in the context of the employment relationship, primary responsibility for the data vis-à-vis the employee remains with the company in the EU. It follows that, where European employees make complaints about violations of their data protection rights and are not satisfied with the results of internal review, complaint, and appeal procedures (or any applicable grievance procedures under a contract with a trade union), they should be directed to the state or national data protection or labor authority in the jurisdiction where the employee works. This also includes cases where the alleged mishandling of their personal information has taken place in the United States, is the responsibility of the US organization that has received the information from the employer and not of the employer and thus involves an alleged breach of the Safe Harbor Principles, rather than of national laws implementing the Directive. This will be the most efficient way to address the often overlapping rights and obligations imposed by local labor law and labor agreements as well as data protection law.

A US organization participating in the Safe Harbor that uses EU human resources data transferred from the European Union in the context of the employment relationship and that wishes such transfers to be covered by the Safe Harbor must therefore commit to cooperate in investigations by and to comply with the advice of competent EU authorities in such cases. The data protection authorities that have agreed to cooperate in this way will notify the European Commission and the U.S. Department of Commerce. If a US organization participating in the Safe Harbor wishes to transfer human resources data from an EU Member State where the data protection authority has not so agreed, the provisions of FAQ 5: The Role of the Data Protection Authorities will apply.[12]

[12] FAQ 5 is at the U.S. International Trade Administration's website at http://export.gov/safeharbor/eu/eg_main_018378.asp.

CONTACT THE CORPORATE & BUSINESS | GAMING PRACTICE

Hinckley Allen's Gaming Practice welcomes the opportunity to speak with you about our services. For more information, please visit hinckleyallen.com/gaming or contact:

Mark Hichar
Partner, Gaming and Co-Chair, International
401-457-5316
mhichar@hinckleyallen.com

William W. Bouton, III
Partner, Chair, Corporate & Business
860-331-2626
wbouton@hinckleyallen.com

Aaron A. Gilman
Partner, Vice-Chair, Corporate & Business
617-378-4324
agilman@hinckleyallen.com

ABOUT HINCKLEY ALLEN

We are a multiservice law firm offering a full range of legal services and pragmatic business advice to regional, national and international clients, with practices including Construction, Corporate, Litigation, Real Estate, and Trusts & Estates. With our longstanding reputation for creating lasting, meaningful business relationships, we are more than just a law firm. We are a law firm that truly and fully engages with our clients.

---

hinckleyallen.com

HINCKLEY ALLEN