JICLT
Journal of International Commercial Law and Technology
Vol. 8, No.1 (2013)

Swiss Information Privacy Law and the Transborder Flow of Personal Data

Sylvain Métille[1]
sylvain.metille@romandie.com

Abstract: Switzerland, like the European Union, has an extensive protection of privacy. An omnibus law, the Data Protection Act, ensures a high level of protection for every data relating to an identified or identifiable person, including legal persons. This Act applies both to data treated inside Switzerland and to data exported abroad. Data can only be transmitted if an adequate level of protection is granted.For countries where the legal framework is not deemed to be sufficient like the U.S., particular contractual clauses are necessary. In order to facilitate the exchange of data, Switzerland and the U.S. have developed a Safe Harbor Framework. Every company certified compatible with the Safe Harbor is automatically recognized as offering the adequate level of protection required under Swiss law.

1. Introduction

To paraphrase the Council of Europe, with the increase in exchanges of personal data across national borders, it is necessary to ensure the effective protection of human rights and fundamental freedom and in particular, the right to privacy and it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples.[2]

Information privacy law, generally known in Europe as data protection law, offers a very different protection on both sides of the Atlantic Ocean. With little simplification, the right to privacy in the U.S. is an aspect of liberty and a right "to be let alone." In contrast, the right to privacy in Switzerland and Europe is an aspect of dignity and a right to be respected. The European continent at first fears the press and the market, when America fears the Government and defends as main value private property and free speech. Finally, the U.S. is attached to an individual's reasonable expectation of privacy, where Swiss and European people consider privacy not only as an individual right but also a social value that needs to be defended by an official data Commissioner.[3]

This paper aims to present the legal protection of information privacy and the current relevant requirements when data is treated in or exported from Switzerland. The analysis is based on the current legislation and does not take into account the early stages of expected modifications of the privacy law in Europe, which are subject to multiple amendments[4].

According to the Swiss legislation, personal data can only be exported if the foreign country offers an adequate level of protection or if sufficient safeguards ensure an adequate level of protection abroad, like particular contractual clauses. As the U.S. is not considered to offer sufficient protection, a Safe Harbor

---

[1] Dr Sylvain Métille, Lecturer at the Faculty of Law and Criminal Justice of the University of Lausanne and at the University of Applied Sciences Western Switzerland, Attorney at Law at id est avocats, Lausanne. This article was mainly written during my time as a visiting scholar at the Berkeley Center for Law and Technology (UC Berkeley). I thank research assistants Jean Perrenoud and Everett Monroe for their valuable help.

[2] *See* Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows, Nov. 8, 2001, C.E.T.S. 181 [hereafter Convention 181].

[3] Francesca E. Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609 (2007); Paul M. Schwartz & Karl-Nikolaus Peifer, *Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?*, 98 CALIF. L. REV. 1925 (2010); *James Q. Whitman, The two western cultures of privacy: dignity versus liberty*, 113 YALE L.J. 1151 (2004).

[4] *See* for the modernization of the Convention 108 the proposal of the Consultative Committee at http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_EN.asp? and for the revision of the Directive 95/46/EC the Commission's proposal and information on the reform at http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm (last visited August 15, 2012). A revision of the Swiss DPA is not expected before 2014.

has been negotiated between the American Federal Trade Commission and the Swiss Federal Data Protection and Information Commissioner. Thus a Swiss company can transmit data to an American company complying with the U.S.-Swiss Safe Harbor Framework without violating the Swiss law.

2. Information Privacy in Switzerland

2.1 In General

In Switzerland, privacy and data protection are granted by the Constitution, the Federal act on data protection (DPA) and similar acts in every Canton. In addition, the European Convention of Human Rights (ECHR)[5] plays a key role in consequence of its self-executing character and its own enforcement body the European Court of Human Rights (ECtHR). The ECHR is considered to be at the same level than the Constitution and the individual rights granted by the Convention can be invoked as constitutional rights before the Swiss courts.

The DPA applies to the processing of data by private persons or federal bodies, and every cantonal act on data protection applies to the processing of data by official bodies of this Canton. Both DPA and cantonal acts are framed by international treaties. The DPA establishes several rights and principles, and the institution of a Commissioner. There are specific rules in DPA about transnational flow of data.

2.2 Constitutional Law

Both the Swiss Constitution and the ECHR establish a right to privacy and provide a similar scope of protection, even though they use different words. The right to privacy is an individual right related to the dignity and autonomy of the human person. It encompasses the idea that everyone can determine what information about his private life should be communicated to others and to what extent.[6]

In the Federal Constitution of the Swiss Confederation, privacy derives mostly from article 13, which says that "everyone has the right to privacy in their private and family life and in their home, and in relation to their mail and telecommunications", and "everyone has the right to be protected against the misuse of their personal data".

Article 13 was introduced in the new Constitution of 1999. Under the previous Constitution of 1874, the right to privacy was part of the right to personal freedom, which was a non-written Constitutional right confirmed by the federal court in 1963.[7] Article 13 covers privacy and information privacy or data protection. The first sentence protects the privacy in general and emphasizes the protection of the person and of his or her living quarters and work space (internal) and his or her communications with others

---

[5] The European Convention on Human Rights (ECHR) is an international treaty under which the member States of the Council of Europe promise to secure fundamental civil and political rights, not only to their own citizens but also to everyone within their jurisdiction. The European Court of Human Rights (ECtHR), a permanent international Court based in Strasbourg known for its progressive and dynamic interpretation of the Convention, enforces the ECHR. It is important to stress that the Council of Europe is an international organization in Strasbourg which comprises 47 countries of Europe and was set up to promote democracy and protect human rights and the rule of law in Europe (http://www.coe.int). This organization is sometimes confused with the European Council (sometimes called the Council of the European Union, http://www.consilium.europa.eu). The European Council is not an international organization but a body of the European Union (EU), and more precisely a regular meeting of the heads of state or executive from the member states of the European Union for the purpose of planning Union policy. 47 States are actually Members of the Council of Europe (and enacted ECHR), while 27 States are member of the European Union. Switzerland is a member of the Council of Europe but not of the European Union (EU).

[6] For comparisons of the American and European notion of privacy see James Q. Whitman, *The two western cultures of privacy: dignity versus liberty*, 113 YALE L.J. 1151 (2004); Bignami, *supra* note 2. For a comparison of the German and American protection of privacy in case of surveillance see Paul M. Schwartz, *German and US Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance*, 54 HASTINGS L.J. 751 (2002); Paul M. Schwartz, *Evaluating Telecommunications Surveillance in Germany: The Lessons of the Max Planck Institute's Study*, 72 GEO. WASH. L. REV. 1244 (2003); Schwartz & Peifer, *supra* note 2; Jacqueline E. Ross, *The Place of Covert Surveillance in Democratic Societies: A Comparative Study of the United States and Germany*, 55 AM. J. COMP. L. 493 (2007).

[7] For personal freedom see Tribunal fédéral [TF] [Federal Supreme Court] Mar. 20, 1963, 89 ARRÊTS DU TRIBUNAL FÉDÉRAL [ATF] I 92, 98 (Switz.); for right of privacy see TF Oct. 21, 1981, 107 ATF Ia 148; PHILIPPE MEIER, PROTECTION DES DONNÉES, 59-78 (2011).

(external). The second sentence establishes the traditional protection of personal data or "information privacy" as it is referred to in the U.S. This informational self-determination right gives every person the basic right to decide what information he wants to share and how.[8]

Article 8 of the European Convention on Human Rights (ECHR)[9] protects the right to respect for private and family life: "Everyone has the right to respect for his private and family life, his home and his correspondence." The European Court of Human Rights (ECtHR) has applied a dynamic and broad interpretation of the Convention. Information privacy is covered by article 8 ECHR.[10]

The Swiss Supreme Court, like the European Court of Human Rights, has refused to give a definitive or exhaustive definition the notion of "private life". It certainly covers the physical and psychological integrity of a person and incorporates the notion of personal autonomy. It also protects a right to identity and personal development, such as the right to establish relationships with other human beings and the outside world. It may also include activities of a professional or business nature.[11]

Fundamental rights limit the power of the State, but they cannot be invoked against other private persons; they do not have a horizontal effect.[12] Citizens are protected from the State by the Constitution and the ECHR, but they are protected from other people only by civil and criminal law. DPA provide civil and criminal remedies against misuse of data.

The exercise of fundamental rights and liberties (like the right to privacy) is not absolute and can be subject to limitations. According to article 36 of the Constitution, a restriction must respect four conditions: it must have a legal basis, it must be justified in the public interest or for the protection of the fundamental rights of others, it must meet the standard of proportionality of means and ends,[13] and there can be no violation of the essence of the fundamental right at stake. The Constitution says the essence of fundamental rights is sacrosanct.[14] Like the Swiss Constitution, the ECHR permits some restrictions in its article 8.2[15]. This can be summarized as the requirements of legal basis, legitimate objectives, necessity and proportionality.

According to this system of rights and the rule of law, there can be no restriction without a statute that expressly permits it. The federal Constitution as well as the ECHR requires a law (clear, sufficiently accessible to the person concerned and foreseeable as to its effects), a public interest, and the respect of proportionality and the essence of the right. Federal bodies may only process personal data if there is a statutory basis for doing so.[16]

---

[8] TF July 9, 2003, 129 ATF I 232, 245-246; TF July 9, 2003, 128 ATF II 259, 268.

[9] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms *adopted* Nov. 4, 1950, E.T.S. 5 [hereinafter ECHR], *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm.

[10] Klass v. Germany, 28 Eur. Ct. H.R. (ser. A) (1978), Malone v. The United Kingdom, 82 Eur. Ct. H.R. (ser. A) (1984). MEIER, *supra* note 7, at 79-85.

[11] *See, e,g.* S. and Marper v. The United Kingdom, App. No. 30562/04 and 30566/04, § 66 , European Court of Human Rights [ECtHR] (2008), *available at* http://cmiskp.echr.coe.int/tkp197/search.asp?skin=hudoc-en. (enter the full App. No. into the Application Number field, and then click Search.) Gillian and Quinton v. The United Kingdom, App. No. 4158/05, §61, ECtHR (2010).

[12] Art. 8, para. 3 of the Swiss Constitution (equality between men and women) is the exception. JEAN-FRANÇOIS AUBERT & PASCAL MAHON, PETIT COMMENTAIRE DE LA CONSTITUTION FÉDÉRALE DE LA CONFÉDÉRATION SUISSE DU 18 AVRIL 1999, 62-63, 311-317 (2003).

[13] The principle of proportionality is mentioned in article 5 of the Swiss Constitution as well and governs all activity of the State. THOMAS FLEINER, ALEXANDER MISIC & NICOLE TÖPPERWIEN, SWISS CONSTITUTIONAL LAW, 39-40 (2005).

[14] CONSTITUTION FÉDÉRALE [CST] [CONSTITUTION] Apr. 18, 1999, RO 101, art. 36 (Switz.). ANDREAS AUER, GIORGIO MALINVERNI & MICHEL HOTTELIER ET AL., DROIT CONSTITUTIONNEL SUISSE II, 79-119 (2006); GIOVANNI BIAGGINI, BV: BUNDESVERFASSUNG DER SCHWEIZERISCHEN EIDGENOSSENSCHAFT UND AUSZÜGE AUS DER EMRK, DEN UNO-PAKTEN SOWIE DEM BGG, 75-109 (2007); ULRICH HÄFELIN, WALTER HALLER & HELEN KELLER, SCHWEIZERISCHES BUNDESSTAATSRECHT, 90-101 (2008); AUBERT & MAHON, *supra* note 11, at 319-331 (2003); RENÉ RHINOW, GRUNDZÜGE DES SCHWEIZERISCHEN VERFASSUNGSRECHTS, 199-206 (2003); RENÉ A. RHINOW & MARKUS SCHEFER, SCHWEIZERISCHES VERFASSUNGSRECHT, 237-245 (2009); WALTER HALLER, THE SWISS CONSTITUTION IN A COMPARATIVE CONTEXT, 157-162 (2009); FLEINER ET AL., *supra* note 12, at 178-182.

[15] "There shall be no interference by a public authority with the exercise of this right except such as 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." ECHR, *supra* note 8, art. 8.2.

[16] LOI FÉDÉRALE DU 19 JUIN 1992 SUR LA PROTECTION DES DONNÉES [LPD] [FEDERAL ACT OF 19 JUNE 1992 ON DATA PROTECTION] [hereinafter DPA] RS 235.1, art. 17. para 1 (Switz.).

2.3 International Law

The ECHR is the most important international source of law and is treated as constitutional law. However, other international treaties, such as the Convention 108 of the Council of Europe or the OECD guidelines are relevant to the extent they inspired and shaped the current legal framework in Switzerland, but there are not self-executing.

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) was adopted in 1981 by the Council of Europe. Forty three countries have ratified the convention and is the first binding international instrument to protect the individual against abuses which may accompany the collection and processing of personal data. The Convention 108 was completed in 2001 by an Additional Protocol regarding supervisory authorities and transborder data flows.[17] Switzerland ratified the Convention in 1997 and enacted it in February 1998. Switzerland also ratified the Protocol in 2007 and enacted it in 2008. Principles contained in the Convention 108 have been integrated into the law of many countries as well as the European Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/EC).[18] The European Directive does not apply to Switzerland, though some provisions shall be very similar under Swiss law as a result of the association agreement to Schengen/Dublin signed by Switzerland[19].

Article 2 of the Protocol requires that each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organization that is not Party to the Convention only if that State or organization ensures an adequate level of protection for the intended data transfer.

According to paragraph 2 of this article, derogation can be granted in two different cases: the first one is if domestic law provides for it because of specific interests of the data subject or legitimate prevailing interests like important public interests. The second one is if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law.[20]

Worth to mention is the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[21] established in 1980 by the Organization for Economic Cooperation and Development (OECD). The Guidelines are nonbinding but they have had a significant impact on the development of national law all over the world. They content eight principles on the procession of personal data, similar to the ones contained in the Convention 108: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.[22]

3. Data Protection Act

The Swiss Confederation is a federative State divided into 26 Cantons. The federal State and the Cantons share law-making competences. The Confederation can legislate regarding criminal law, civil law, and regarding the organization of the federal authorities and administration, while the Cantons legislate regarding the organization of their cantonal authorities and administration.[23] Reflecting the split in authority, the Federal Act on Data Protection (DPA)[24] applies only to the processing of data pertaining to natural and legal persons by private persons or federal bodies,[25] while every Canton has a cantonal act on

---

[17] Convention 181, *supra* note 3.
[18] 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, 1995 O.J. (L 281). The Council of Europe is an international organization in Strasbourg which comprises 47 countries, while the European Council (sometimes called the Council of the European Union) is a body of the European Union (EU) in Brussels.
[19] MEIER, *supra* note 7, at 101-104.
[20] Jean-Philippe Walter, *Communication de données personnelles à l'étranger*, in DIE REVISION DES DATENSCHUTZGESETZES, 102, 102-115 (Astrid Epiney & Patrick Hobi eds., 2009); MEIER, *supra* note 7, at 85-88.
[21] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).
[22] MEIER, *supra* note 7, at 91-93.
[23] Conseil Fédéral, Message concernant la Loi fédérale sur la protection des données FF II 421, 432-433 (1988); MEIER, *supra* note 7, at 117-119.
[24] DPA, RS 235.1.
[25] *Id.* art. 2.

data protection that applies to the processing of data by cantonal bodies. Thus, DPA establishes the scope of federal powers and cantonal acts cover areas outside of that scope.

The Swiss Government proposed a first draft for the usual consultation procedure in 1984. Many interested parties commented the draft. Four years late, and having taken into account some of these comments, the Federal Council submitted the final draft to Parliament.

The Federal Act on Data Protection has been adopted by Parliament on June 19, 1992 and it came into force on July 1, 1993. DPA aims to protect the privacy and the fundamental rights of persons when their data is processed. It is an omnibus law that regulates private activities and public (federal) activities.[26] The DPA was partially revised in March 2006 and it introduces a duty of information towards data subjects when collecting personal data that are either especially sensitive or concern a personality profile.

In July 2000 the European Commission stated Switzerland is considered as providing an adequate level of protection for personal data transferred from the European Community[27].

Under Swiss law, information relating to an identified or identifiable person is called personal data (sometimes data or personal information).[28] This includes both natural and legal persons. This definition is very similar to the one provided by the Convention 108, yet Convention 108 does not protect legal persons.

The DPA extends the personality rights granted by the Swiss Civil Code (SCC).[29] The Swiss Civil Code provides a general protection of legal personality (art. 28ss): "Any person whose personality rights are unlawfully infringed may apply to the court for protection against all those causing the infringement. An infringement is unlawful unless it is justified by the consent of the person whose rights are infringed or by an overriding private or public interest or by law."[30]

Swiss law ensures a broad protection of privacy and is fully compatible with the European Convention on Human Rights and Convention 108. It offers sometimes even more protection to corporate entities. The Federal Act on Data Protection covers most of the situations and even requires adequate protections for data transmitted abroad. The DPA sets a series of principles like proportionality, purpose, evidence, consent, security, correctness and consent and provides different cause of action like correction of data, limitation of disclosure, or destruction of data.

3.1 Rights provided by the Data Protection Act

a) Core principles

Data processing must be lawful,[31] carried out in good faith, and proportionate. Proportionality covers three elements: ability (the means used are adequate to obtain the targeted end), necessity (choice of means that cause the intrusion or damages) and strict meaning proportionality (balance between interference with private life caused by the proposed means and the potential planned benefits).[32]

Personal data may only be processed for the purpose indicated at the time of collection, that is obvious from the circumstances, or that is provided for by law.[33]

Evidence is a key requirement added in 2008: the collection of personal data and in particular the purpose of its processing must be obvious to the data subject[34]. A duty to provide information about the

---

[26] MEIER, *supra* note 7; URS MAURER-LAMBROU & NEDIM PETER VOGT, BASLER KOMMENTAR ZUR DATENSCHUTZGESETZ (2008); DAVID ROSENTHAL & YVONNE JÖHRI, HANDKOMMENTAR ZUM DATENSCHUTZGESETZ (2008).

[27] Commission issued Decision 2000/518, of July 26, 2000, pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland O.J. (L 215) 1 (CE).

[28] DPA art. 3, para. a. MEIER, *supra* note 7, at 197-203.

[29] Code Civil [CC] [Civil Code] Dec. 10, 1907, RS 210, art. 28ss (Switz.).

[30] REGINA E. AEBI-MÜLLER, PERSONENBEZOGENE INFORMATIONEN IM SYSTEM DES ZIVILRECHTLICHEN PERSÖNLICHKEITSSCHUTZES UNTER BESONDER BERÜCKSICHTIGUNG DER RECHTSLAGE IN DER SCHWEIZ UND IN DEUTSCHLAND, 1-180 (2005); STÉPHANE BONDALLAZ, LA PROTECTION DES PERSONNES ET DE LEURS DONNÉES DANS LES TÉLÉCOMMUNICATIONS, 146-156 (2007); HEINZ HAUSHEER & REGINA E. AEBI-MÜLLER, DAS PERSONENRECHT DES SCHWEIZERISCHEN ZIVILGESETZBUCHES, 148-234 (2008); HENRI DESCHENAUX & PAUL-HENRI STEINAUER, PERSONNES PHYSIQUES ET TUTELLE, 159-224 (2001).

[31] Not illegal regarding another law.

[32] TF, July 13, 2004, 130 ATF II 425, para. 5.2 (Switz.). MEIER, *supra* note 7, at 267-281.

[33] DPA art. 4, para. 3. MEIER, *supra* note 7, at 281-286.

[34] DPA art. 4, para. 4. MEIER, *supra* note 7, at 274-281.

collection of data is required for federal bodies or for private bodies when private bodies collect sensitive personal data or personality profiles.[35]

Where the consent of the data subject is required for the processing of personal data, such consent is valid only if given voluntarily on the provision of adequate information. Additionally, consent must be given expressly in the case of processing of sensitive personal data or personality profiles.[36]

DPA requires that personal data be protected against unauthorized processing through adequate technical and organizational measures.[37]

Correctness is a principle and a cause of action. Anyone who processes personal data must make certain that it is correct. He must take all reasonable measures to ensure that data that is incorrect or incomplete in view of the purpose of its collection is either corrected or destroyed. The DPA allows any data subject to request that incorrect data be corrected.[38]

b) Legal claims and procedure

Among the remedies available to the plaintiff are: that data processing is stopped, that no data be disclosed to third parties, or that personal data be corrected or destroyed. These are in addition to the general remedies relating to the protection of the personality contained in articles 28ss of the Civil Code (prohibition of a threatened infringement, order to cease an existing infringement, declaration that an infringement is unlawful if it continues to have an offensive effect) and damages (tort, articles 41ss of the Code of Obligations).[39]

Articles 34 and 35 of the DPA contain some criminal provisions. On complaint, private persons are liable to a fine if they breach their obligations to provide information, to register or to cooperate with the Commissioner, or if they breach professional confidentiality.[40]

Finally, the DPA gives a right to information. Any person may request information from the controller of a data file as to whether data concerning them is being processed. The controller of a data file must notify the data subject of all available data concerning the subject in the data file including available information on the source of the data, the purpose of and if applicable the legal basis for the processing, the categories of the personal data processed, the other parties involved with the file, and the data recipient. The information must normally be provided in writing and is free of charge.[41]

c) Cross-border flow of data

As a core principle, article 6 of the DPA states that personal data may not be disclosed abroad if the privacy of the data subjects would be seriously endangered thereby, in particular due to the absence of legislation that guarantees adequate protection. The law presumes that the danger will realize due to the lack of an adequate legislation. Violation of article 6 of the DPA is a privacy harm *per se*. DPA does not completely forbid the disclosure of data if the protection provided by the law of the target country is not deemed to be sufficient, but only in particular situations or when additional warranties are given.[42]

In the absence of legislation that guarantees adequate protection, personal data may be disclosed abroad in four situations; First, if the data subject has consented in the specific case, the processing is directly connected with the conclusion or the performance of a contract, and the personal data is that of a contractual party; Second, if disclosure is essential in the specific case in order either to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts; Third, if disclosure is required in the specific case in order to protect the life or the physical

---

[35] DPA arts. 14, 18a. Sensitive personal data is data on religious, ideological, political or trade union-related views or activities; health, the intimate sphere or the racial origin; social security measures; criminal proceedings and sanctions. A personality profile is a collection of data that permits an assessment of essential characteristics of the personality of a natural person. MEIER, *supra* note 7, at 345-360.
[36] DPA art. 4 para. 5. MEIER, *supra* note 7, at 316-344.
[37] DPA art. 7. MEIER, *supra* note 7, at 297-316. Articles 8-12 and 20-23 of the Ordinance to the Federal Act on Data Protection of June 14, 1993, give more details about the technical and organizational measures.
[38] DPA art. 5. MEIER, *supra* note 7, at 287-297.
[39] DPA arts. 5 para. 2, 15, 25. MEIER, *supra* note 7, at 563-601.
[40] DPA arts. 34, 35.
[41] DPA art. 8. MEIER, *supra* note 7, at 361-419.
[42] DPA art. 6. Walter, *supra* note 20, 120-134. ROSENTHAL & JÖHRI , *supra* note 26, at 130-175. MEIER, *supra* note 7, at 436-476.

integrity of the data subject.; Fourth, if the data subject has made the data generally accessible and has not expressly prohibited its processing.

Additionally, personal data may also be transmitted abroad if sufficient safeguards, in particular contractual clauses, ensure an adequate level of protection abroad or if disclosure is made within the same legal person or company or between legal persons or companies that are under the same management, provided those involved are subject to data protection rules that ensure an adequate level of protection. In these two cases the Federal Data Protection and Information Commissioner must be informed of the safeguards and the data protection rules.

d) Federal Data Protection and Information Commissioner

The DPA also establishes the role of Federal Data Protection and Information Commissioner (FDPIC). The Commissioner supervises compliance by federal authorities with data protection regulations and advises private persons on data protection matters. He has investigatory powers and can address recommendations as well. If the addressee challenges the Commissioner's recommendation, the Commissioner can defend it in the courtroom.[43]

In matter of cross-border disclosure the Commissioner must be informed of the safeguards contained in particular contractual clauses[44] or the data protection rules within a company[45] that ensures an adequate level of protection abroad.

The FDPIC has to provide an expert opinion on the extent to which foreign data protection legislation guarantees adequate protection, to cooperate with domestic and foreign data protection authorities and finally to advise private persons on data protection matters.[46]

3.2 International export of data

Cross-border flow of data or international flow of data refers to every kind of transmission of data out of the Sovereignty of one State to be treated in another State or international/supranational organization. This includes import, export, and transit of data.[47]

Under Swiss law, if personal data is made generally accessible by means of automated information and communications services, such as the internet, for the purposes of providing information to the general public, this is not deemed to be transborder disclosure.[48] The publication of a website is not an international transfer of data, but collection of information that is not generally accessible on the website, such as cookies and IP addresses, is an international transfer of data.[49]

As soon as data is treated in Switzerland, DPA must be respected regardless of the national or international origin of the data.[50] DPA does not only apply to data treated in Switzerland but also to data exported from Switzerland. Article 6 of the DPA requires legislation that guarantees adequate protection to allow data to be disclosed abroad. The Federal Data and Information Commissioner keeps an up-to-date list of countries with adequate protection.[51] Only a very few number of countries protects corporate privacy and are adequate for those data.[52] For private persons, the contracting parties to the Convention 108 and the additional Protocol are presumed to grant an adequate level of protection. U.S. is among the countries that do not have the legal framework to insure a sufficient protection.

To make up for the absence of an adequate protection, safeguards can be granted in a contract. Different models of contract are typically recognized to offer a sufficient protection, such as the Model

---

[43] MEIER, *supra* note 7, at 602-623.
[44] DPA art. 6 para. 2(a) .
[45] DPA art. 6 para. 2(g).
[46] DPA arts. 31 para. 1(c)-(d), 28.
[47] Walter, *supra* note 20, at 116-117. MEIER, *supra* note 7, at 441-445.
[48] ORDONNANCE RELATIVE A LA LOI FÉDÉRALE SUR LA PROCECTION DES DONNÉES [OLPD] [ORDINANCE TO THE FEDERAL ACT ON DATA PROTECTION] June 14, 1993, RS 235.11, art. 5 (Switz.).
[49] MEIER, *supra* note 7, 443-444.
[50] Amtliches Sammlung der Entscheide des schweizerischen Bundesverwaltungsgericht [BVGE] [Federal Administrative Court], Mar. 30, 2011, docket no. A 7040/2009, para. 5 (Switz.), *available at* http://www.bvger.ch/medien/medienmitteilungen/00695/index.html?lang=de.
[51] Lies des Etats [List of States] *available at* http://www.edoeb.admin.ch/themen/00794/00827/. The fact that a country is not included on the list does not mean that it does not provide an adequate level of protection.
[52] Austria, Denmark (partially), Italy, Liechtenstein, Argentina (partially).

contract of the Council of Europe,[53] the European standard contractual clauses,[54] and the Commissioner's model contract for the outsourcing of data processing abroad[55].

3.3 U.S.-Swiss Safe Harbor Framework

3.3.1 A Framework

As a result of the previously described different privacy approaches, the Swiss DPA could have significantly restricted the ability of U.S. companies to engage in a range of international transactions as the ability to Swiss companies to deal with American organizations. However, there was no way to change one or the other legal system to make them more compatible.[56]

The Swiss Federal Data Protection and Information Commissioner and the U.S. Department of Commerce developed a Safe Harbor Framework in 2008, similar to the Safe Harbor negotiated a few years earlier between the U.S. Department of Commerce and the EU Commission, yet U.S.-Swiss and U.S.-EU Safe Harbor Frameworks are completely independent.[57]

The U.S.-Swiss Safe Harbor Framework is not a treaty but rather a framework made of an exchange of letters from the U.S. Department of Commerce, from the Federal Trade Commission and from the Department of Transportation on the U.S. side and an answering letter from the Federal Data Protection and Information Commissioner to the U.S. Department of Commerce on the Swiss side. Both letters from the U.S. Department of Commerce and FDPIC enclosed five annexes: U.S.-Swiss Safe Harbor Principles (Annex I), Frequently Asked Questions (Annex II), Safe Harbor Enforcement Overview (Annex II), a Memorandum by the Department of Commerce on Damages for Breaches of Privacy, Legal Authorizations and Mergers and Takeovers in U.S. Law (Annex IV) and the U.S. government bodies recognized by Switzerland empowered to investigate complaints (Annex V).

This very atypical and confusing framework is the result of two drastically different ways to approach and regulate privacy. There is no obligation to commit to the Safe Harbor, neither from a Swiss perspective, nor a U.S. perspective. The Safe Harbor is nothing more than one of the tools a company can use.

The U.S.-EU Safe Harbor Framework is signed by the Commission and this is uncertain whether the Safe Harbor is binding for national data privacy agencies.[58] There were also some discussions about the authority of the European Commission to negotiate the Safe Harbor and the absence of a formal finding of non-adequate protection[59]. This question is not relevant for Switzerland: contrary to the U.S.-EU Safe Harbor Framework, the U.S.-Swiss Safe Harbor Framework is signed by the FDPIC itself and he has authority to provide an expert opinion on the adequate protection of foreign legislation and to cooperate with foreign data protection authorities.

The Safe Harbor is a self-certification process. It relies on a voluntary mechanism of a public commitment being made by the U.S. organization to conform to the seven defined principles and renewed every year. The compliance with the published Privacy policy and the principles mentioned above may occur either through a self-assessment program or an outside assessment program (third-party). However this is a mere declaration and no independent party checks the compliance with the principles and the declared policy.

---

[53] The Model contract to ensure equivalent protection in the context of transborder data flows made jointly by the Council of Europe, the Commission of the European Communities and International Chamber of Commerce (1992).
[54] Commission Decision 2001/497, of June 15, 2001, on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Under Directive 95/46/EC, 2001 O.J. (L 181) 19 (EC); Commission Decision 2004/915, of December 27, 2004, as Regards the Introduction of an Alternative Set of Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, 2004 O.J. (L 385) 74 (EC); and Commission Decision 2010/87, of February 5, 2010, on Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries Under Directive 95/46/EC, 2010 O.J. (L 39) 5 (EU).
[55] Swiss Transborder Data Flow Agreement (for outsourcing of data processing).
[56] Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUS. L. REV. 717, 739-740 (2001).
[57] Even though the form used for self-certifying compliance with the U.S.-Swiss Safe Harbor Framework is identical to the one used for self-certifying compliance with the U.S.-EU Safe Harbor Framework.
[58] A directive is generally not binding and a transposition into national law is needed. The Commission intends to substitute a Regulation (which, if enacted, makes it directly applicable in every Member State) for the Directive 95/46/EC. *See supra* note 4.
[59] Reidenberg, *supra* note 56 at 741-742.

Under Swiss law, an adequate level of protection is automatically acknowledged for any company that has joined the U.S.-Swiss Safe Harbor Framework. This is one possible way that a Swiss company can choose to comply with article 6 of DPA.[60] The Safe Harbor Framework only addresses the question of the legislation that guarantees adequate protection. Transmitting data to a certified company does not exempt the Swiss company to comply with other provisions of DPA such as the right to information or the rules pertaining to the processing by third parties.

Joining the U.S.-Swiss Safe Harbor Framework is a simple and cheap way for an American company to comply with the DPA. The Swiss company only has to check if the American company is currently listed within U.S. organizations that have self-certified to the U.S.-Swiss Safe Harbor Framework.

3.3.2 Seven principles

The U.S.-Swiss Safe Harbor Framework is made of seven principles: notice, choice, onward transfer, security, data integrity, access, and enforcement.

A clear and understandable notice must be provided about the purpose of the data collection. Individuals must have the opportunity to opt-out if data is to be disclosed to a third party or to be used for a purpose which is "incompatible" with the purpose for which it was collected. For sensitive information, an opt-out is not sufficient and the individual has to opt-in.

Notice and choice principles also apply if information is disclosed to a third party (onward transfer). The third party must be subject to the DPA, subscribe to the Safe Harbor Framework or provide at least the same level of privacy protection by a written agreement.

Security measures are necessary and particularly reasonable precautions that must be taken to protect data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. Once data integrity has been established, reasonable steps should be taken to ensure that data is reliable for its intended use, accurate, complete, and current.

Individuals must have a right to access and to correct information collected about them.

Organizations may satisfy the enforcement requirements (verification, dispute resolution, and remedy) through various means. Organizations can comply with private privacy programs that incorporate the Safe Harbor Principles into their rules and that include effective enforcement mechanisms; comply with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or commit to cooperating with the Swiss Data Commissioner or authorized representatives.

3.3.3 Safe Harbor's Government Enforcement

Swiss enforcement for exporting data without ensuring an adequate level of protection is different than U.S. enforcement for not respecting the Safe Harbor.

For example if a company established in Switzerland transfers data to the U.S. without sufficient safeguards, it would be a violation of the DPA, and would be prosecuted in Switzerland. The compliance of a U.S. company who receives the exported data is not the responsibility of the Swiss company as long as the U.S. company is certified compliant with the Safe Harbor, the same as when data is exported to a country that offers an adequate protection. A Swiss Company can only be held responsible when a company or a country notoriously disrespects the rules.[61]

In addition to the private sector enforcement mentioned in the seven principles, the Federal Trade Commission[62] may provide overarching government enforcement of the Safe Harbor Privacy Principles, yet the underlying legal authority of the FTC may be questionable.[63] The failure to comply with the Safe Harbor Privacy Principles is anyway actionable under federal or state law prohibiting unfair and deceptive acts.

The FTC has sued only a few entities regarding their compliance with the U.S.-EU Safe Harbor Framework. Most of these actions were because the company represented that it held current certifications to the Safe Harbor program when the company had allowed their certifications to lapse.[64]

---

[60] For other possibilities see part 0.
[61] MEIER, *supra* note 7, at 449-450.
[62] Or depending on the industry sector and the slip of legal competences another U.S. government agencies, or the states.
[63] Reidenberg, *supra* note 56 at 740-741.
[64] *See, e.g., FTC Settles with Six Companies Claiming to Comply with International Privacy Framework*, FEDERAL TRADE COMMISSION, http://www.ftc.gov/opa/2009/10/safeharbor.shtm (last visited July 15, 2012).

From a Swiss perspective, the lack of enforcement by the FTC does not mean an inadequate protection; the safeguards granted in a contract do not benefit from a specific enforcement by a governmental agency.[65]

Recently the FTC brought their first substantive Safe Harbor violation action against Google regarding its implementation of its social network, Google Buzz, in 2010. The settlement resolves the charges that Google used deceptive tactics and violated its own privacy promises to consumers and in particular their certifications of the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks.[66]

3.3.4 Limitations

While the U.S.-Swiss Safe Harbor Framework is a bridge between different legal conceptions, the Framework is not fully equivalent to the Swiss requirements. As such, the U.S.-Swiss Safe Harbor Framework suffers several limitations. Among other limitations, it does not apply to every company, it covers only data of private persons, and the certification is timely limited.

Only organizations that are subject to the jurisdiction of the Federal Trade Commission (FTC) and U.S. air carriers and ticket agents that are subject to the jurisdiction of the Department of Transportation (DoT) may participate in the Safe Harbor. Banks, credit unions, telecommunication common carriers, labor associations, non-profit organizations, certain insurance activities, and other organizations are not eligible.

Data about corporations are not covered by the Safe Harbor. Because legal entities enjoy a similar privacy protection under Swiss law as individuals, an adequate protection must be guaranteed by another way if there is personal data of a corporation among the exported data.

The certification is only valid for one year (but can be renewed) and a certification for the Swiss Safe Harbor is not valid for the EU Safe Harbor and vice versa. Finally, the self-certification mentions the privacy policy of the company, but does not indicate how effectively the company respects its own privacy policy.

4. Conclusion

Switzerland as Europe and the U.S. do not share the same conception of privacy and consequently the level of protection that should be devoted to it. However, all three share economic interests. The Safe Harbor Framework is a possibility among others to transfer data into the U.S. in full respect of the Swiss DPA. For a Swiss company, this is one of the easiest ways to comply with DPA and particularly for small companies who want to avoid drafting to many important contracts. This is not always the best method, but it is an easy one and worth knowing about. In addition, the Safe Harbor certification can demonstrate for an American company an interest to offer a higher standard of privacy protection to its customers. Because this is only a self-certification, additional measures should be taken to demonstrate the company's full compliance with its own privacy policy.

.* * * * *

Cite as: Métille, Sylvain. Swiss Information Privacy Law and the Transborder Flow of Personal Data. *Journal of International Commercial Law and Technology*, Vol.8 No.1 (January, 2013)

[65] *See* part C.

[66] *FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network*, FEDERAL TRADE COMMISSION, http://www.ftc.gov/opa/2011/03/google.shtm (last visited July 15, 2012); Google, Inc., F.T.C. File no. 102 3136 (*available at* http://www.ftc.gov/os/caselist/1023136).