GDPR on the Swiss Territory. Cooperation with European Authorities and Enforcement of Monetary Fines

Benhamou, Yaniv; Jacot-Guillarmod, Emilie

www.jusletter-it.eu

Yaniv Benhamou / Emilie Jacot-Guillarmod

GDPR on the Swiss Territory

Cooperation with European Authorities and Enforcement of Monetary Fines

Der Beitrag analysiert die Umsetzungsfragen in der Schweiz in Bezug auf die EU-Datenschutz-Grundverordnung (DSGVO) (Verordnung 2016/679, anwendbar ab dem 25. Mai 2018), insbesondere die grenzüberschreitende Zusammenarbeit zwischen Schweizer juristischen Personen oder dem Eidgenössischen Datenschutzbeauftragten und EU-Aufsichtsbehörden sowie die Durchsetzung der Sanktionen und Bussgelder gegenüber Schweizer juristischen Personen sowohl in der EU als auch in der Schweiz. (ah)

Kategorie: Beiträge
Region: Schweiz
Rechtsgebiete: Datenschutz

Zitiervorschlag: Yaniv Benhamou / Emilie Jacot-Guillarmod, GDPR on the Swiss Territory, in: Jusletter IT 24. Mai 2018

Contents

Introduction

[Rz 1] The extent of the scope of the General Data Protection Regulation (GDPR) (in particular its extra-territorial scope) and the obligations arising from the text of said regulation have been dealt with extensively by legal authorities[1]. However, questions of enforcement, in particular the cooperation with the European authorities and the implementation of European sanctions, are less addressed topics[2].

1. Cooperation with European Authorities

1.1. Direct Transmission of Information from the Swiss Company to the European Authorities

[Rz 2] Cooperation with European supervisory authorities is likely to increase with the GDPR. In addition to the administrative fines, whose execution in Switzerland will be discussed below (2.2), European supervisory authorities may conduct investigations (e.g. requesting all type of information and carry out audits) and impose corrective measures (e.g. imposing a modification, temporary or permanent limitation of processing activities) (Article 58). Swiss companies will

1 See Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, Die EU-Datenschutzgrundverordnung und ihre Auswirkungen auf die Schweiz, March 2018 (https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2018/Leitfaden%20zur%20DSGVO%20Stand%20Mai%202018.pdf.download.pdf/Die_EU_DSGVO_und_ihre_Auswirkungen_auf_die_Schweiz_DE_mai2018.pdf); Sebastien Fanti, Le nouveau Règlement général sur la protection des données et la Suisse : le nœud gordien de la double régulation et le fragile substrat législatif, Expert Focus 2017, 856. More specifically on the territorial scope, cf. Daniel Ennöckl, in: Gernot Sydow (ed.), Europäische Datenschutzgrundverordnung, Handkommentar, Baden-Baden 2017, Article 3, p. 251; David Vasella, Zum Anwendungsbereich der DSGVO, in: digma 4/2017, 221.

2 See however Motion 16.3752 by Fiala Doris filed on September 28, 2016, and accepted by the Federal Council on November 9, 2016, encouraging talks between the Federal Council and the European authorities to improve cooperation between Swiss and European authorities in view of a good application of respective data protection legislations. See also Manuel Bergamelli, Die Auswirkung der neuen DSGVO auf die Schweiz, in: Jusletter April 30, 2018.

also have the duty to notify the supervisory authority of the violation of personal data (Article 33). Swiss companies will tend to cooperate, in particular in order to avoid administrative fines and/or in order to avoid the supervisory authority to seize judicial authorities (Article 58 para. 5).

[Rz 3] Swiss companies may thus be required to cooperate directly with the supervisory authorities. Such cooperation raises the question of whether such cooperation is a prohibited act within the meaning of Article 271 of the Swiss Criminal Code (SCC). At first glance, conditions seem to be fulfilled. The transmission of information for the purposes of a foreign proceeding (civil, criminal or administrative) would constitute an act that falls within «*the responsibility of a public authority*». Such act would be executed «*without authorization*» in the absence of a mutual assistance procedure or authorization delivered by a Swiss authority and it would be executed «*on Swiss territory*», even if the information are communicated via the EU representative or the Data Protection Officer (DPO) domiciled in the EU, as it is sufficient that only part of the relevant acts are carried out in Switzerland[3]. Upon further review, a distinction shall be made between various scenarios.

[Rz 4] In our opinion, the act performed by a Swiss company (in particular the production of documents following a security breach or an investigation of the European authority) should not constitute a prohibited act within the meaning of Article 271 para. 1 SCC, as long as it only concerns the company targeted by the request for information[4]. According to several authors, Article 271 para. 1 SCC aims at protecting Swiss sovereignty (by preventing the execution of acts on Swiss territory which fall within «*the responsibility of a public authority*», regardless of the characteristics of the entity acting, official or not, or the qualification of the act abroad) but not at preventing a person located in Switzerland from defending his interests abroad[5].

[Rz 5] This approach based on the defence of interests of the person targeted by the measures is, however, subject to the following temperaments:

- the possibility of freely producing documents is limited to foreign procedures in which the person located in Switzerland is a party and is defending its own interests. It will be thus necessary to carefully review the person from whom the information is requested. When the required information is actually requested from a third party (e.g. an affiliate that has delegated processing activities to another affiliate), the production of documents will then, in principle, have to be carried out by means of mutual assistance[6]. It will also be necessary to pay attention to the person who requests the information, as it may not only be directly an authority, but also be indirectly a third-party acting as a long arm of the authority (e.g.

3 Philipp Fischer/Alexandre Richa, in: Alain Macaluso/Laurent Moreillon/Nicolas Queloz (eds.), Commentaire romand du Code pénal II, Article 111–292 CP, Basel 2017 (hereinafter cited as CR CP II-Author), Article 271 CP N 37. It should be specified that Article 271 para. 1 SCC would not be applicable, if all information to be provided are located abroad, e.g. at the representative's or DPO's UE premises, due to the lack of activity on Swiss territory.

4 CR CP II-Fischer/Richa, N 23. See also the four decisions of 2016 regarding an authorisation request addressed to the Federal Department of Justice and Police (DFJP), in which the DFJP recalled that the production of documents in a civil proceeding abroad is, in principle, not an act falling within the responsibility of a public authority: VPB 2016.3, 32–37 consid. 9; VPB 2016.7, 56–61 consid. 9; VPB 2016.8, 62–70 consid. 11.

5 CR CP II-Fischer/Richa, Article 271 CP N 22–32; Markus Husmann, in: Marcel Alexander Niggli/Hans Wiprächtiger (eds.), Basler Kommentar Strafrecht II, Article 111–392, Basel 2013 (hereinafter cited as BSK Strafrecht II-Author), Article 271 N 32.

6 CR CP II-Fischer/Richa, N 25; BSK Strafrecht II-Husmann, Article 271 N 32; Philippe Vladimir Boss, L'autorisation d'exécuter un acte pour un État étranger dans la pratique récente, Revue de l'avocat 2017, p. 77 ss, p. 81.

an attorney-at-law or a third-party at the request of an authority)[7]. The critical point is that the Swiss entity must not behave «*as an authority*»[8]. Article 271 para. 1 SCC does not apply to a person who acts in a recognizable manner as a private person (e.g. without presenting himself as a representative of a foreign authority or without resorting to particular procedural arrangements required by the rules applicable to the foreign procedure)[9]. When the information is requested by a third-party, e.g. by the EU representative or the DPO at the request from a European authority, it will also be more beneficial to use the path of mutual assistance;

- any confidential duties remain reserved: the production of information must indeed be carried out in compliance with any confidentiality obligations (e.g. Article 47 of the Swiss Federal Law on Banks and Savings Banks, Article 43 of the Swiss Federal Law on Stock Exchanges and Securities Trading, and Article 162 or 273 SCC, data protection)[10]. Swiss companies will thus have to guarantee the confidentiality, in particular bank secrecy, professional or contractual, in particular by communicating only categories of personal data or anonymous personal data[11]; and
- the Swiss Federal Office of Justice (OFJ) does not share this approach based on the defence of interests, at least not in the field of international mutual assistance in civil matters, for whom the decisive criterion for qualifying an act falling within «*the responsibility of a public authority*» is that the refusal to cooperate may lead to criminal or administrations sanctions[12]. Transposed to data protection, this reasoning would lead to the conclusion that any cooperation with European authorities (the production of documents following a security breach or an investigation of the European authority) would fall under the application of Article 271 para. 1 SCC. This reasoning must, however, be rejected in our view on the grounds that is has no legal basis[13] and has been issued for the field of international mutual assistance in civil matters, and is thus not necessarily transposable to mutual assistance in data protection.

[Rz 6] In view of the approach adopted by the Swiss Federal Office of Justice, the uncertainty created by Article 271 para. 1 SCC in its application in the field of data protection, particularly considering the different definitions of an act falling within «*the responsibility of a public authority*», and the evolution of international cooperation[14], it is desirable that Switzerland offers a clear

---

7 Cf. ATF 114 IV 128 consid. 2c: the Swiss Supreme Court held that the offence under Article 271 SCC was given in the case of an attorney-at-law which proceeded in Switzerland to the audition of a witness in order to use the content of said audition before a foreign court.

8 Cf. VPB 2016.3, N 9 («*wie ein Gericht*») or VPB 2016.4, N 11 and VPB 2016.8, N 11 («*wie ein Gerichtsorgan*»), cited by CR CP II-Fischer/Richa, article 271 N 24.

9 CR CP II-Fischer/Richa, N 19. See, however, the contrary approach which considers that preparatory acts in view of a future act falling within the responsibility of a public authority for a future trial abroad (e.g. interview of a possible witness to assess his knowledge of the facts) are not subject to Article 271 para. 1 SCC. Contra CR CP II-Fischer/Richa, Article 271 N 16, considering that the criteria of «*preparatory act*» is not relevant, as it cannot be excluded that the information collected will be used at a later stage in a proceeding abroad.

10 CR CP II-Fischer/Richa, Article 271 N 23.

11 Modality expressly provided in case of security breach (article 33 al. 2 GDPR).

12 OFJ, Lignes directrices sur l'entraide judiciaire internationale en matière civile, 12. In favor of this approach: Boss (note 6), p. 80, for whom the four decisions quoted in n.4 make it possible to release such a key definition.

13 CR CP II-Fischer/Richa, Article 271 CP N 27: specify that otherwise any person responding to an authority with a power of coercion would carry out an «act under public authorities».

14 Which lead in particular the Swiss authorities to adopt special rules in the field of international cooperation in the finance and banking sector (Article 42 ss LFINMA) and individual authorisation (see model decision of 3 July

legal framework of international data protection cooperation and that the competent authorities issue general or individual authorisations allowing the transmission of information, or negotiate an agreement on mutual administrative assistance[15]. Meanwhile, prior to such clarification, the cautious approach requires that Swiss companies ask for an authorisation prior to any cooperation with the European authorities in order to avoid committing an act prohibited by Article 271 para. 1 SCC.

1.2. Transmission of Information from the Swiss DPO to the European Authorities

[Rz 7] With regard to the extra-territorial scope of the GDPR, a certain number of Swiss companies will be subject to simultaneous supervision by the European authorities and the Federal Data Protection and Information Commissioner (FDPIC)[16]. Increased cooperation between the FDPIC and European authorities will be consequently desirable. The European authorities may also wish to obtain certain information directly from the FDPIC.

[Rz 8] As a preliminary point, we note that, in practice, informal collaboration between Swiss and European authorities is common in many areas. More specifically, the exchange of general information between authorities on their activities or their projects does not require any specific legal basis[17]. By contrast, any exchange of confidential information is a matter of formal mutual assistance and requires in principle a legal basis, in accordance with the principle of legality. Mutual assistance may rely on domestic law (federal or cantonal), or on an international convention[18]. As it stands, Swiss law provide no general legal basis (domestic or conventional) governing mutual assistance. *De lega lata*, in addition, there is no special international convention on administrative mutual assistance in the field of data protection[19].

[Rz 9] The Swiss Federal Act on Data Protection (FADP) contains general rules on the transfer of information by federal bodies (Article 19 et seq. FADP) and limits itself to assigning the task of

2013 in tax matters and the draft legislation «*loi sur la collaboration et la protection de la souveraineté*» of 20 February 2013, which purported to set out more clearly the balance of interests to be assessed by the Swiss authority prior to the issuance of the authorisation within the meaning of Article 271 para. 1 SCC, later abandoned on the ground that the difficulties experienced in the international cooperation may be solved without a formal act).

15 See the parliamentary motion entitled «To avoid duplications with respect to data protection», adopted by the Swiss National Council (*Conseil national*) on 16 December 2016 and by the Swiss Council of States (*Conseil des Etats*) on 17 February 2017 (https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163752%20Page).

16 Rapport de la Commission des institutions politiques du 12 janvier 2018 (https://www.parlament.ch/centers/kb/Documents/2016/Rapport_de_la_commission_CIP-E_16.3752_2017-01-12.pdf); Fanti (note 1), p. 859.

17 Pierre Moor/Alexandre Flückiger/Vincent Martenet, Droit administratif – Volume I : Les fondements, 3ème éd., Berne 2012, p. 169.

18 Id., p. 170.

19 Unlike international standards (e.g. IOSCO MMoU, IAIS MMoU, OECD model agreement on exchange of information in tax matters) or bilateral agreements between the FINMA and the foreign authorities in the finance and banking sector. This may change with the P-LPD, which give the Federal Council authority to conclude international treaties in international cooperation (Article 61 P-LPD). It should be noted that the communication of information to European authorities may also be based on international assistance in criminal matters, in particular on certain international conventions binding Switzerland and the EU, e.g. the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 and the Convention on Cybercrime of 23 November 2001. The analysis of the corresponding provisions is beyond the scope of this contribution.

collaborating with foreign data officers to the FDPIC (Article 31, para. 1, let. c FADP)[20]. FDPIC can thus collaborate with foreign authorities and provide them with information, in accordance with the general principles of state activity[21], especially the principle of proportionality (Article 5 para. 2 of the Swiss Federal Constitution) which prohibits fishing expeditions[22], and data protection.

[Rz 10] According to Article 19 para. 1 FADP, the communication of personal data by federal bodies requires in principle a legal basis. As an exception, the FADP allows federal bodies to communicate personal data notwithstanding the absence of a legal basis in certain cases, in particular (1) when the communication is indispensable to the recipient for the fulfilment of its statutory task (Article 19 para. 1 letter a FADP) or (2) when the data subject has consented to the transfer in the concrete case (Article 19 para. 1 letter b FADP):

- As regards the first ground, it is not sufficient for the communication to facilitate or improve the performance of the applicant authority's task. The absence of data transmission must completely prevent the requesting authority from fulfilling its statutory task in a concrete case[23]. In our view, a strict approach is appropriate in assessing the necessity of the communication. Such assessment should take into account the means at disposal of the requesting authority to obtain the information directly from the data subject. In view of the broad powers conferred on the EU supervisory authorities by the GDPR, it may be expected that the transmission of data by the Swiss Federal Commissioner will rarely be indispensable within the meaning of Article 19 para. 1 let. a FADP.
- By contrast, it is likely that Swiss entities subject to both the FADP and the GDPR will consent to the transmission to European authorities of some of their data in the possession of the Swiss Federal Commissioner, in order to avoid having to submit the same information several times to the various competent authorities.

[Rz 11] The general rules on cross-border data communication (Article 6 FADP) also apply to the exchange of information with foreign authorities. This should not raise difficulties as European legislation ensures an adequate level of protection abroad.

[Rz 12] In principle, the person concerned by this procedure has the right to oppose the transfer of data by asserting a legitimate interest (Article 20 FADP). However, this right is not always implemented in practice. Indeed, case law does not require systematically a formal decision to transfer information, in which case the person concerned will not always be aware of it in advance[24]. That being said, it is to be expected that the FDPIC will pay particular attention to the respect of the rights of the individuals concerned under the application of the FADP, whose proper application is under its supervision. Legal authorities generally hold that the principle of specialty (i.e. the fact that the requesting authority may use the information provided only in the framework of the procedure underlying the request for assistance) applies in the case of administrative mutual assistance[25]. Therefore, according to Swiss law as it stands, the FDPIC

20 Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales, FF 2017 6565, 6710 (hereinafter cited as Message P-LPD).

21 Moor/Flückiger/Martenet (note 17), p. 968 ss.

22 ATF 129 II 484.

23 Decision of the Swiss federal administrative court A-6320/2014 of 23 August 2016 consid. 5.8.

24 ATF 136 II 23; Moor/Flückiger/Martenet (note 17), p. 995.

25 Moor/Flückiger/Martenet (note 17), p. 992 s.; Thierry Amy, Entraide administrative internationale en matière bancaire, boursière et financière, Thèse, Lausanne 1998, p. 407.

has in principle to ensure that the European authorities do not use the information provided for purposes other than those of data protection[26].

[Rz 13] The draft for a revised Swiss Federal Data Protection Act (P-FADP) provides in details the administrative assistance between the FDPIC and the foreign authorities in charge of data protection (Article 49 P-FADP). The exchange of information and data protection between the FDPIC and a foreign authority in charge of data protection would be in particular subject to the requirement of reciprocity and confidentiality (Article 49 para. 1 P-FADP)[27]. In our opinion, the European authorities will in principle fulfil these conditions, in particular with regard to the relevant provisions of the GDPR (Article 50 GDPR)[28]. In our view, Article 49 P-FADP constitutes a *lex specialis* in relation to the general provision on the communication of personal data by federal bodies (Article 32 lit. f P-FADP). In particular, Article 49 para. 3 P-FADP provides for the prior information of the data subject only when the data transmitted are likely to contain professional, manufacturing or business secrets and to the extent that this does not require disproportionate efforts. In our view, this more restrictive provision takes precedence over the general right of the data subject to oppose any transfer of his personal data (Article 33 P-FADP)[29], and allows the transmission of data without prior notification when no professional, manufacturing or business secret is in jeopardy. This evolution is questionable in view of the right to be heard by the person concerned[30]. Finally, we note that the P-FADP provides explicitly that the foreign authority may use the information exchanged only as part of a procedure on which the request for assistance is based, in accordance with the principle of specialty (Article 49 para. 1, let. b P-FADP).

[Rz 14] In the view of the foregoing, the P-FADP will allow the FDPIC to transmit information more widely to its foreign counterparts, especially in the absence of consent from the relevant data subject. It also clarifies the modalities of mutual assistance and the possible use of the information transmitted. That being said, the potential resulting limitation of the relevant data subject's right is unfortunate in our view.

2. Enforcement of Monetary Fines

2.1. Enforcement in the EU

(A) Enforcement against a Representative in the EU?

[Rz 15] Controllers and processors based outside of the EU, but subject to the GDPR within the meaning of GDPR 3 § 2 (extra-territorial scope), shall designate a representative in the EU in

26 By analogy with the stock market and financial areas, cf. Amy (note 25), p. 407.

27 These principles are also found in other areas of cooperation, in particular cooperation in finance and banking sector (article 42 al. 2 let. a and b LFINMA) which provides however more specific rules, in particular for client information («*procédure-client*»): the administrative procedure applies (article 42a al. 2 LFINMA), but with some flexibilities, such as the transmission without prior notification to the client when such prior notification could compromise the administrative assistance purposes (in particular in case of urgency, e.g. risk of collusion or altering the evidence) (article 42a al. 4 LFINMA). Biba Homsy, Nouvelles dispositions en matière de coopération internationale : ouverture ou contrôle de la FINMA?, in: Jusletter Avril 18, 2016, 13.

28 Cf. also par. 61 Preamble of the GDPR.

29 This provision corresponds in substance to the current Article 20 FADP, see Message P-LPD, 6698 s.

30 By analogy to bank and financial matters, cf. Andrea Opel, Amtshilfe ohne Information der Betroffenen – eine rechtsstaatlich bedenklich Neuerung, in ASA 83 (2014/2015), p. 265 ss.

writing (Article 27)[31]. The representative (i.e. an individual or legal entity established in one of the Member States where the data subjects, whose personal data are processed, are located) will act on behalf of the controller or the processor represented for all issues related to processing and compliance with GDPR. It/he will perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities for the purposes of ensuring compliance with GDPR.

[Rz 16] If the intention of the European authorities to have a point of contact in the EU is understandable, various points remain open. GDPR states, in the recitals and without more details, that «*the designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation but such representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor*»[32]. This possible application of enforcement proceedings towards the representative raises the question of the scope of its liability.

[Rz 17] Towards the supervisory authorities (external relationships), the following points are relevant:

- if the European authorities require the representative to provide information about the controller/processor, the Swiss authorities may consider that the controller/processor is in breach of Article 271 para. 1 SCC, according to the approach of the OFJ mentioned above (pursuant to which the relevant criteria for defining an act falling within «*the responsibility of a public authority*» (*acte relevant des pouvoirs publics*) within the meaning of Article 271 para. 1 SCC depends on possible sanctions in case of non-cooperation) and if the controller/processor delivers information to the representative who/which in turn delivers the information to the European authorities. Consequently, controller/processor shall ensure that the production of information does not qualify as a prohibited act within the meaning of Article 271 para. 1 SCC, i.e. pending an established practice or formal confirmation that the approach considered by the Swiss authorities is the one explained above based on the defence of interests (and not based on the possible sanction attached to the non-cooperation adopted by the Swiss the Federal Office of Justice), to ask an authorisation from the Swiss competent authority; and
- if the European authorities issue a monetary fine against the controller/processor, it is expected that the responsibility of said representative will be limited to representation (not including liability). As the recital states, however, that the representative is «*subject to enforcement proceedings in the event of non-compliance by the controller or processor*» without detailing whether these proceedings are limited to representation and excluding liability and monetary fines, we cannot exclude that supervisory authorities will seek to enforce sanctions directly against the representative, namely if it has substantial assets in the EU[33].

---

31 Article 27 para. 2 GDPR provides that this obligation does not apply to a «*processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing*».

32 Consid. 80.

33 By contrast, Manuel Klar/Jürgen Kühling, in: Jürgen Kühling/Benedikt Buchner (eds.), Datenschutz-Grundverordnung, Kommentar zur DSGVO, München 2017, Article 27 DSGVO N 17; Bergamelli (note 2), 8, considering that the monetary fines do not apply against the representative by a reasoning a contrario based on Article 83 para. 4 let. a GDPR (which lists all obligations of the controller and processor and which may lead to monetary fines of up to EUR 10 mio or 2% of the worldwide turnover.

Such liability would be qualified as an objective vicarious liability (*responsabilité objective du fait d'autrui*) as the representative would be liable solely because of the acts conducted by the controller/processor without being able to be released from liability. The representative would in turn likely claim indemnification from the controller/processor for the prejudice suffered. This raises the question of internal relationships and a possible indemnification clause to be included in the mandate contract between the representative and the controller/processor.

[Rz 18] Towards the controller/processor (internal relationship), parties will conclude a written contract:

- if there is a choice of Swiss law, the parties will conclude a mandate contract (or a service agreement). It is advisable to provide the scope of representation and allocation of responsibility precisely. In this respect, one can think of an indemnification clause in favour of the representative subject to the statutory limitation of liability (e.g. if the representative acts against the instructions given by the controller/processor and by the supervisory authorities). If there is also a choice of courts in Switzerland, the claim arising from the indemnification clause will be enforced before the Swiss courts directly[34]; and
- if the choice of courts is abroad, the claim arising from the indemnification clause will be enforced before the foreign courts first, then recognized and enforced before the Swiss courts pursuant to the Lugano Convention (LC)[35].

(B) Shared Liability between several Entities (e.g. Joint Controllers, or Controllers-Processors)?

[Rz 19] When several entities infringe the GDPR simultaneously (e.g. affiliates of the same group qualified as joint controllers, or controller and processor), they may be deemed to be jointly liable. European authorities may address requests to each entity jointly or separately and in particular, define whether each entity is liable for the entire damage or only for the portion of damage caused by each party's contribution (causation principle). This question (joint or limited liability and causation principle) will depend on the local applicable law.

[Rz 20] Assuming that the local applicable law is similar to Swiss law, distinction will be made between the entities infringing the GDPR with knowledge of the other party's infringements (so-called «*wrongful cooperation*», «*coopération fautive*»), in which case each entity will be jointly liable for the entire damage, and the entities infringing the GDPR without knowledge of the other party's infringements, in which case each entity will have a liability limited to the portion of damage caused by each party's contribution (causation principle)[36].

[Rz 21] Usually, each entity knows or is aware of the other party's processing activities (e.g. when they act as joint controllers, which define the purposes of processing activities jointly, or when they act as processors upon instructions of the controller) and would be jointly liable for the entire damage. Nevertheless, other situations may be contemplated where each entity acts separately

34 See Section 2.2(E) below.

35 Id.

36 Vincent Perritaz, La solidarité : un monde imparfait, REAS 2018, p. 63 ss: in the first case, the terms «*perfect solidarity*» (*solidarité parfaite*) within the meaning of Article 50 CO are used and, in the second case, the terms «*imperfect solidarity*» (*solidarité imparfaite*) within the meaning of Article 51 CO are used.

from the other entity, i.e. without knowledge of the other party's infringement (e.g. when an affiliate of a group of companies becomes the centralized entity processing the personal data, hence the sole controller) and would be only liable for the portion of damage caused by each party's contribution (causation principle).

2.2. Enforcement in Switzerland

(A) Introduction

[Rz 22] As set forth above, EU data protection authorities are likely to have various means of enforcement against foreign entities on the EU territory. They may reasonably be expected to favour these approaches over enforcement in a third country. Nevertheless, European authorities will have to seek enforcement of their decisions in Switzerland in certain circumstances. Such may be the case for instance in the event that the relevant company's assets are located in Switzerland, that the company is under no obligation to designate a representative in the EU pursuant to Article 27 GDPR[37] or that it has breached this obligation. Based on the principles of territoriality and sovereignty, foreign authorities are generally prohibited from carrying acts of public authority on Swiss territory[38]. Accordingly, foreign authorities are not entitled to act directly in Switzerland[39], but have to seek recognition and enforcement by Swiss authorities.

[Rz 23] Enforcement of European supervisory authorities' decisions on the EU territory may also give rise to related disputes between the European representative and its foreign principal or between jointly responsible entities. In particular, in the event that sanctions are enforced against the European representative or against a jointly responsible entity located in the EU, such representative or entity may seek indemnification from the Swiss company.

[Rz 24] This section provides an analysis of the proceedings, which may be available for the enforcement in Switzerland of EU authorities' decisions on the one hand, and of indemnification claims of the EU representative and/or jointly responsible entity against the Swiss company on the other hand.

(B) Legal Nature of Decisions Based on GDPR

[Rz 25] The applicable enforcement proceedings in Switzerland vary depending on the field of law (i.e. administrative, civil or criminal) to which, from a Swiss law perspective[40], the relevant decision pertains.

[Rz 26] Upon first review, decisions taken by European authorities in application of the GDPR (i.e. measures taken by an authority in a specific case which influence the legal position of the

37 Pursuant to Article 27 par. 2 GDPR, foreign entities which process data of EU residents only occasionally are exempted from the obligation to designate a representative, provided that they do not process certain specific categories of data on a large scale.

38 Moor/Flückiger/Martenet (note 17), p. 156.

39 Please refer to Section 1.1 above regarding criminal sanctions, which may apply in the event of unauthorised cooperation to acts of public authority by foreign authorities on Swiss soil.

40 As such, the GDPR text referring to «*administrative fines*» is therefore not decisive.

addressee[41]) qualify as administrative decisions within the meaning of Swiss law. We also note that, in Swiss domestic matters, sanctions imposed by Swiss administrative authorities pertain to administrative law[42].

[Rz 27] That being said, pursuant to court precedents, sanctions imposed by administrative authorities may be criminal in nature[43]. The criteria for qualifying a sanction as administrative or criminal, as well as the very notion of an administrative sanction, are debated among legal scholars[44]. Failing a clear distinction, we cannot exclude that sanctions based on GDPR be considered as criminal in nature. In any event, such abstract analysis would be of little practical interest, as international assistance in criminal matters laws set their own criteria to determine whether a decision falls within their respective scope of application. Accordingly, this section analyses whether the sanctions set forth in GDPR may be enforced in accordance with international assistance in criminal matters laws.

[Rz 28] Data protection pertains in principle to public law. Nevertheless, data protection may give rise to private law claims[45]. Accordingly, cross-border enforcement of data protection rules is governed by private international law under certain circumstances[46]. More specifically, litigation between the EU representative and its Swiss principal or between jointly responsible entities pertains to civil law, as it involves individuals and/or private entities. Therefore, this section also analyses if decisions based on GDPR and/or decisions taken within the context of related litigation may be enforced in accordance with Swiss international private law rules.

(C) Administrative Assistance

[Rz 29] As a matter of Swiss law, there is no general statute governing the recognition and enforcement of foreign administrative decisions.

[Rz 30] There is no specific legal basis for the recognition and enforcement in Switzerland of decisions based on foreign data protection laws. Thus, as it stands, Swiss law does not provide for the recognition and enforcement of decisions taken under the GDPR by EU authorities as a matter of administrative assistance.

[Rz 31] In turn, the P-FADP does not provide a legal basis for the recognition and enforcement of decisions taken under the GDPR either. The administrative assistance measures, which may

41 Cf. article 5 PA. See also Jean-Baptiste Zufferey, La décision administrative – Un alibi au service de tous les intérêts, in: Benoît Bovay/Minh Son Nguyen (eds.), Mélanges Pierre Moor, Théorie du droit – Droit administratif – Organisation du territoire, Berne 2005, p. 637 ss, p. 639.

42 Article 1 LPD.

43 ECHR, Engel and others vs the Netherlands, No. 5100/71 of 8 June 1976.

44 For a detailed discussion, see e.g. Marcel Alexander Niggli/Christof Riedo, Quasi-Strafrecht, Strafrecht im engeren und weiteren Sinne und «Sozialethisches Unwerturteil», in: Marc Amstutz/Inge Hochreutener/Walter A. Stoffel (eds.), Die Praxis des Kartellgesetzes im Spannungsfeld von Recht und Ökonomie, Zurich 2011.

45 Decision of the Swiss federal administrative court A-7040/2009 of 30 March 2011 c. 5.1 ss (Google Street View); André Thalmann, Zur Anwendung des schweizerischen Datenschutzgesetzes auf internationale Sachverhalte, in: sic! 2007, pp. 337 ss, p. 338. Please note that as such, the involvement of administrative authorities does not exclude the application of international private law rules. Swiss legal scholars argue for instance that the Swiss federal data protection and information commissioner may elect applicable law in accordance with Article 139 of the Swiss Federal Private International Law Act (PILA), similarly to the injured party (David Rosenthal/Yvonne Jöhri, Handkommentar zum Datenschutzgesetz, Zurich 2018, Article 29 LDP N 7; question left undecided in: Decision of the Swiss federal administrative court A-7040/2009 of 30 March 2011 c. 5.5.2 [Google Street View]).

46 Decision of the Swiss federal administrative court A-7040/2009 of 30 March 2011 c. 5.1 ss (Google Street View), Thalmann (note 45), p. 338.

be granted by the Federal Commissioner under the P-FADP, do not include the enforcement of foreign authorities' decisions (including in particular sanctions) in Switzerland. While some political steps have been taken towards the conclusion of a Swiss-EU agreement on coordination in the field of data protection, this process remains at a very early stage[47]. In the near future, the adoption of a legal basis for the enforcement of decisions under the GDPR as a matter of mutual administrative assistance thus seems unlikely.

(D) International Assistance in Criminal Matters

[Rz 32] The Swiss Federal Act on International Mutual Assistance in Criminal Matters (EIMP)[48] provides for the recognition and enforcement of foreign decisions in criminal matters in Switzerland, under certain conditions. In principle, a decision falls within the scope of application of EIMP provided that it qualifies as a decision in criminal matters according to the criteria of the Engel case law[49]: a sanction is criminal in nature in the event that, alternatively, (1) national law classifies it as such, or (2) the nature of the offence or the severity of the potential sanction denotes its criminal character[50]. EU law classifies the sanctions imposed under the GDPR as administrative fines (Article 83 seq. GDPR). However, in view of the gravity of the potential penalties, which may reach 4% of the total annual worldwide turnover for the financial year preceding the infringement, they are, in our view, criminal in nature as per the Engel case law criteria[51].

[Rz 33] The recognition and enforcement in Switzerland of a foreign decision in criminal matters presupposes that the law of the requesting State permits recourse to the courts with respect to the relevant decision (Article 1 para. 3 EIMP). Swiss practice is rather generous in this respect, to the extent that Swiss authorities and courts grant mutual assistance also at the preliminary stage of the proceedings in the requesting State, even if a non-judicial authority is in charge of the proceedings at this stage[52]. Pursuant to court precedents, mutual assistance may namely be granted to administrative authorities, provided that such administrative authorities intervene prior to referral to the competent courts[53].

[Rz 34] Notwithstanding the foregoing, the Swiss Supreme Court requires that the offences giving rise to the request for mutual assistance be punishable by judicial authorities of the requesting State. Accordingly, mutual assistance in criminal matters may be granted only if the foreign proceedings result in the referral of accused persons to a competent court[54]. In this respect, we note that EU supervisory authorities impose themselves the sanctions set forth in the GDPR.

---

47 Parliamentary motion (note 15); discussed in: Fanti (note 1), p. 859.

48 It should be noted that the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 does not provide a legal basis for the recognition and enforcement of foreign criminal decisions.

49 Gerhard Fiolka, in: Marcel Alexander Niggli/Stefan Heimgartner (eds.), Basler Kommentar Internationales Strafrecht, Basel 2015 (hereinafter cited as BSK Internationales Strafrecht-Author), Article 1 EIMP N 36.

50 ECHR, Engel and others vs the Netherlands, No. 5100/71 of 8 June 1976.

51 Our analysis is in line with judicial guidance with respect to similar sanctions in the field of antitrust law, cf. ECHR, Menarini Diagnostics S.R.L. vs. Italia, No. 43509/08 of 27 September 2011; ATF 139 I 72.

52 See Article 11 EIMP, pursuant to which a «*defendant*» under the Act is any person under suspicion, which is subject to criminal proceedings or on whom a sentence has been imposed; Swiss Federal Court decision 1A.326/2005 of 1 March 2006 c. 2.2; BSK Internationales Strafrechet-Fiolka, Article 1 EIMP N 36; Laurent Moreillon, Commentaire romand Entraide internationale en matière pénale, Basel 2003, Article 1 N 67.

53 ATF 113 Ib 257; ATF 109 Ib 47; Swiss Federal Court decision 1A.326/2005 of 1 March 2006 c. 2.2.

54 Swiss Federal Court decision 1A.326/2005 of 1 March 2006 c. 2.2.

The potential subsequent appeal before a judicial authority[55] does not, in our view, meet the requirements of the abovementioned Swiss federal case law. Failing recourse to the courts within the meaning of Article 1 para. 3 EIMP, sanctions imposed under the GDPR cannot, in our view, benefit from international mutual assistance in criminal matters in Switzerland.

[Rz 35] Even if the Swiss authorities were to develop a more flexible approach and be satisfied with the possibility of an appeal before a judicial body, the enforcement in Switzerland of a foreign criminal decision is subject to the requirement of dual criminality (Article 94 para. 1 let. b EIMP): the act or omission sanctioned by the foreign authority has to also constitute an offence under Swiss law. The scope of application of the sanctions under the GDPR significantly exceeds that of the criminal sanctions under the FADP and, albeit to a lesser extent, under the P-FADP. Therefore, even assuming that sanctions imposed in accordance with the GDPR may benefit from mutual assistance in criminal matters in Switzerland[56], Swiss authorities are likely to refuse the enforcement of sanctions imposed thereunder in a significant number of cases, due to the lack of dual criminality.

[Rz 36] In any event, Swiss authorities enforce a foreign sanction only up to the maximum penalty provided for by Swiss law for the same offence (Article 94 para. 3 EIMP), in accordance with the *lex mitior* principle[57]. Consequently, even if mutual assistance in international criminal matters were granted in Switzerland and if, in the concrete case, Swiss law punished the conduct sanctioned by the European authorities, the fine imposed in Switzerland could not exceed CHF 10,000 under currently applicable law (Article 34 s. FADP *cum* Article 106 SCC). Subject to the outcome of parliamentary debates, this maximum will be increased to CHF 250,000 upon the P-FADP coming into force (Article 54 seq. P-FADP). Thus, the risk for Swiss entities against which direct enforcement on Swiss territory is sought by the EU supervisory authorities is in any event well below the maximum penalties provided for by the GDPR (i.e. up to EUR 20,000,000 or 4% of annual worldwide turnover).

(E) International Private Law

[Rz 37] The Lugano Convention governs the recognition and exequatur in Switzerland of European judgments in civil and commercial matters, whatever the nature of the court or tribunal (Article 1 para. 1 cum Article 62 LC). We note that the field of data protection is not excluded from the scope of the Convention (Article 1 al. 2 LC a contrario). As regards GDPR, our analysis differentiates between the implementation of (1) decisions taken by European supervisory authorities (in particular sanctions), (2) decisions taken in respect of possible indemnification claims by the EU representative against its Swiss principal, and (3) decisions taken in respect of possible indemnification claims by European entities against a Swiss co-responsible entity.

[Rz 38] As regards sanctions imposed by EU supervisory authorities, it should be noted that administrative authorities» decisions may be recognised and enforced in accordance with the Lugano Convention, provided that they relate to civil and commercial matters within the mean-

55 EU Member States have to implement appropriate procedural safeguards, including effective judicial remedy, with respect to the sanctions imposed by supervisory authorities (Article 83 para. 8 GDPR).

56 In our view, such is not the case pursuant to existing case law, see above paragraphs of this Section.

57 BSK Internationales Strafrechet- Youssef/Heimgartner, Article 94 EIMP N 22.

ing of the Convention[58]. Pursuant to applicable case law, the notion of civil and commercial matters must be interpreted broadly. Where the legal relationship involves a governmental body, the Lugano Convention applies if that governmental body acts similarly to a private person or entity. By contrast, the Lugano Convention does not apply in the event that the authority acts in its capacity as holder of public authority[59]. EU data protection authorities exercise regulatory, decision-making and sanctioning powers[60] when imposing the measures (in particular sanctions) set forth in the GDPR. In these circumstances, their decisions do pertain to a civil or commercial matter within the meaning of the Lugano Convention. Therefore, recognition and enforcement of sanctions imposed by the EU supervisory authorities in accordance with the Lugano Convention is not an option.

[Rz 39] As regards disputes between the EU representative and its Swiss principal will in principle relate to a contract. Matters related to a contract fall within the scope of application of the Lugano Convention (Article 5 para. 1 LC). As previously mentioned[61], the EU representative and the Swiss entity may agree to submit their disputes to Swiss courts (Article 23 LC). In this case, the representative will assert any indemnification claims directly before the Swiss courts and no cross-border enforcement will be necessary. In the event that the parties choose to submit their disputes to the courts of an EU Member State, decisions rendered by such elected courts (Article 23 LC) are automatically recognised (Article 33 seq. LC) and may be enforced (Article 38 seq. LC) in Switzerland in accordance with the Lugano Convention.

[Rz 40] A potential shared responsibility[62] will in principle arise between entities bound by contract (e.g. contract between controller and processor or agreement on joint processing responsibilities). Reference may therefore be made to the immediately preceding paragraph in the event that there is a contractual choice of court. Failing such a choice of court, the courts of the place of performance of the obligation in question has jurisdiction by default (Article 5 para. 1 let. a LC), subject to the special provisions on service contracts (Article 5 par. 1 let. b LC)[63]. Any indemnification claims will in arise from the defendant's (i.e. the Swiss party's) breach of its obligations. We may assume that the place of performance of these obligations will regularly be located in Switzerland, in which case the dispute will take place directly before Swiss courts and no cross-border enforcement will be necessary.

58 Matthias Lerch/Thomas Rohner, in: Christian Oetiker/Thomas Weibel (eds.), Basler Kommentar Lugano-Übereinkommen, Basel 2016, Article 1 LC N 37.

59 ECJ, Decision C-29/76 of 14 October 1976, LTU Lufttransportunternehmen GmbH & Co. KG vs. Eurocontrol; ATF 124 III 436 c. 3.

60 As regards the notion of public authority acts, please refer e.g. to Stéphane Voisard, L'auxiliaire dans la surveillance administrative – Du droit bancaire et financier au droit administratif général, in: Arbeiten aus dem Iuristischen Seminar der Universität Freiburg Schweiz, 333, p. 75 ss, N 160 ss.

61 See Section 2.1(A) above.

62 See Section 2.1(B) above.

63 With respect to service contracts, the courts of the place where, under the contract, the services were provided or should have been provided have jurisdiction by default (Article 5 para. 1 let. b LC). In our view, the contract between the controller and the processor will in principle qualify as a service contract within the meaning of the Lugano Convention.

Conclusion

[Rz 41] The extra-territorial scope of the GDPR (and related obligations) has already been extensively discussed. Its enforcement in Switzerland, however, has been less commented and will be foreseeably complex.

[Rz 42] A first relevant topic is the enforcement of monetary fines provided in the GDPR. Such fines will not be directly enforceable in Switzerland. This being said, one cannot exclude an indirect enforcement of such monetary fines, either through a presence in the EU (e.g. the representative in the EU or the entity jointly liable for the processing activities, such as a joint controller), which will then claim civil indemnification against the Swiss entity.

[Rz 43] Another relevant topic is the cooperation with European authorities, in particular the right for a Swiss controller/processor to cooperate in light of the prohibition to carry out activities on behalf of a foreign state within the meaning of Article 271 para. 1 SCC. In this respect, we recommend a flexible approach, which allows for a Swiss controller/processor to defend its own interests abroad, in compliance with any applicable confidentiality duties.

[Rz 44] Generally, there is a lack of clarity with respect to future interactions between Swiss and European authorities, the consequences for Swiss controllers/processors subject to a double regulation, GDPR and the Swiss data protection act. For legal security purposes, a prompt clarification by our Swiss authorities would be welcome.

Dr. Yaniv Benhamou is a lecturer in intellectual property law at the University of Geneva and an attorney admitted to the Geneva bar. In his practice as an attorney, he advises clients with regard to commercial law, in particular to technology, media & telecoms and data protection law.
Emilie Jacot-Guillarmod is an attorney admitted to the Geneva bar. She advises clients on international and domestic transactions, with a particular focus on M&A transactions, financings and data protection law.
The authors would like to sincerely thank their colleagues Philippe Fischer and Téo Genecand, for their very helpful review of this contribution and shared insights, as well as Ms. Nathalie Aymon and Ana Andrijevic for their much appreciated help with the translation of this text into English.