www.jusletter-it.eu

Philippe Gilliéron

Towards GDPR Compliance as a Best Practice: a Primer for Swiss SMEs

Over the last years, privacy concerns have significantly increased, and the recent adoption of the GDPR in May 2018 coupled with the Cambridge Analytica scandal now give cold sweats to most companies. SMEs are struggling to find their way in a field they have little understanding of (if any), and find it hard to know where to start from. This paper aims at providing them some basic information and checklist to start building a privacy management program without incurring significant expenditures or being a privacy expert.

Category: Articles
Region: Switzerland
Field of law: Data Protection

Citation: Philippe Gilliéron, Towards GDPR Compliance as a Best Practice: a Primer for Swiss SMEs, in: Jusletter IT 26 September 2018

ISSN 1664-848X, https://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Contents

I. Introduction

[Rz 1] In a recent CEDIDAC Bulletin, Sylvain Métille put under scrutiny Art. 3 of the General Data Protection Regulation (GDPR) and the issue to know under which conditions a Swiss entity may or not be subject to the GDPR[1]. As the author acknowledges, no matter the answer to that question, the standards set out in the GDPR are likely to soon be regarded as best practices which, although not amounting to legal obligations, may well be part of the due diligence expected from data controllers in terms of privacy management.

[Rz 2] This due diligence does not only apply to multinational companies, but to any company processing personal data, thus including small and medium enterprises (SMEs). This due diligence is all the more important at a time when companies increasingly use cloud-based services to benefit from the flexibility and scalability offered by these resources, thus partially losing control over their data. Truth however is that, while multinational companies may have the resources, both from a human and financial standpoints, to support their efforts towards the achievement of a GDPR compliant level, such is not the case of SMEs.

[Rz 3] Common grounds for pushback may typically include statements such as: «I have limited resources and budget», «I do not understand what this GR... whatever is about», «I am new to privacy and do not know anything», «I cannot find any checklist that would meet my needs».

[Rz 4] Truth is that the very low level of understanding of privacy related matters within SMEs (sometimes even fairly big ones) make it difficult to transpose the approach used within multinational companies to such companies, even in a simplified way. Tools do exist, and the need for companies to comply with GDPR led to significant developments within the legaltech industry in the last two years in that area. While several providers now compete to win it all[2], their pricing model however demonstrate that their primary target remain multinational companies that have

1 Sylvain Métille, *Le Règlement general sur la protection des données et la Suisse*, Bulletin CEDIDAC n° 72 (April 2018).

2 See for instance, among others: Anonos, Avepoint, DataGuidance, Evidon, Henley Business School, Nymity, OneTrust, RADAR, Redgate Software, Thomson Reuters or TrustArc.

the expertise and financial resources to afford such tools. There is little doubt that few SMEs will afford such luxury.

[Rz 5] Consequently, another methodology has to be adopted to demonstrate the efforts undertaken by SMEs to take into account privacy requirements into their day-to-day business practices.

[Rz 6] This short paper aims at providing a practical guide to enable SMEs to start implementing privacy management activities through their organization without having to be a privacy expert. Pragmatic in its approach, this paper provides a generic overview meant for newcomers in this field, and should thus not be considered as a scholarly piece. Footnotes and references will be limited to the strict minimum.

II. Footprint towards the Setting up of Privacy Management within SME

[Rz 7] Setting up a privacy management program that triggers some privacy awareness within a SME can be achieved without having to hire resources or being a privacy expert. Basic steps consist of the following ones:

A. Data Mapping

1. Mapping

[Rz 8] A primary step will consist of finding out the data processed by your company. This step is important, as it only is after having assessed the type of data that you process that you will be in a position to decide upon the next steps.

[Rz 9] The extent to which personal data are being processed will obviously depend upon your business model, and consumer facing companies involved in e-commerce for instance are likely to process a significantly larger amount of data than a company involved in B2B. No matter your business model, you will in any case process personal data related to your employees. In short, one finds it hard to imagine a company that would not process any personal data.

[Rz 10] In today's world, a company is unlikely to fully control its data processing end-to-end. This means that, at some point, you are likely to have hired vendors to process your data, for instance as a CRM provider (salesforce for instance) or for payroll purposes.

[Rz 11] As a result, to map your data properly, which will typically be done on an excel- or spreadsheet[3], it will be key to understand the type of data you process (consumer, employee, vendors, else), their categories (name, first name, email, phone, etc.), the reason for processing such data (i.e. the purpose, which can be to enable payment to your employees for instance), by whom such data are being processed (do you have full control or use vendors), where such processing takes place (this matters as any processing taking place outside of EEA will require special safeguards), and for how long such data are being retained. This last point is likely to

[3] Some data protection authorities offer templates, that might be considered appropriate or further tailored to your needs: https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles or https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/ (all websites last visited on 13 June 2018).

trigger difficulties, as it has been largely ignored so far by most companies, be they multinational ones or SMEs.

[Rz 12] Depending upon the size of your company, mapping your data will likely require to work with the operational and business units of your company, such as HR, customer service, security, procurement, legal, marketing and sales, i.e. all departments that process personal data or impact such processing.

2. Privacy Impact Assessments

[Rz 13] Once carried out, this mapping may serve as a basis for maintaining a future inventory of any new systems, projects, etc. that would involve data processing, similar to the one required by Art. 30 GDPR.

[Rz 14] This is the point to state that the GDPR makes a distinction between the information to be collected for record purposes, and the ones to be collected when a data protection impact assessment (DPIA) within the meaning of Art. 35 GDPR is required. Suffice it to say that the requirements to perform a DPIA are fairly restrictive and should be the exception rather than the rule for most companies that are subject to the GDPR; such will only be the case when «*the processing is likely to result in a high risk to the rights and freedoms of natural persons*», such as in the case of automated decision making processes, processing of special categories of data (such as health related), or a systematic monitoring of a publicly accessible area on a large scale (such as CCTV).

[Rz 15] In practice, the launch of a new project for companies subject to the GDPR should start with a risk assessment (also sometimes referred to as criticality assessment), followed by a privacy impact assessment, which consist of some basic intake questions enabling to maintain an inventory for record purposes in accordance with Art. 30 GDPR. In cases when the requirements set out under Art. 35 GDPR are met, a DPIA shall then, and only then, be carried out[4]. For Swiss companies that are not subject to the GDPR, DPIAs do – at least for the time being – not come into play.

B. Privacy Policy and Notices

1. Policies and Notices

[Rz 16] Data privacy policy and notices are sometimes mixed for one another, but are not interchangeable.

---

4 On the question of « *high risk*», see notably: *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes or Regulation 2016/679 (wp248 rev. 01)* (Adopted on 4 April 2017 as last Revised and Adopted on 4 October 2017), as well as, among others: CIPL, *Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR* (21 December 2016), at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf, as well as CIPL, *Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's «Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of Regulation 2016/679» adopted on 4 April 2017* (19 May 2017), at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_wp29s_guidelines_on_dpias_and_likely_high_risk_19_may_2017-c.pdf. The CNIL also provides a valuable portal related to privacy impact assessments, including guidelines and templates, see: https://www.cnil.fr/en/privacy-impact-assessment-pia.

[Rz 17] A data privacy policy consists of the baseline foundation of your company meant to describe the organization's handling practices of personal data. It will tell employees what they may do with personal data, how, and is therefore internally focused. A privacy policy may typically contain sections as to its scope (type of information, who the policy applies to), a policy statement (expected behavior and consequences of non-compliance), the protection and destruction standards as well as the relevant contact details.

[Rz 18] A data privacy notice is a statement made to a data subject that will describe how the organization collects, uses, retains, and discloses their personal data. Unlike the policy, it is thus externally facing, telling notably customers what the organization does with their personal data. A data privacy notice will typically consist of the following sections[5]: (i) the type of data collected (what) (ii) the purpose of such collection (why) (iii) the retention period (how long), (iv) the recipients with whom you share the data and the reasons for such sharing (with whom), (v) the location of such processing and potential transfer to third countries of such data (where), (vi) the technical and organizational measures in place to ensure the confidentiality, integrity and authenticity (CIA) of the data, (vii) the data subject rights with regards to such data and (viii) contact details in case of any question.

[Rz 19] In addition to these elements, it will be important to find out the lawful basis for processing the data, which will typically consist of (i) consent, (ii) legitimate interest, (iii) performance of a contract or (iv) a legal obligation. Taking into account that lawful basis for processing is important, as opting for one or another may trigger some difference, notably if your entity is submitted to the GDPR. We shall briefly comment on these below.

[Rz 20] To comply with all these requirements may prove lengthy and burdensome. This may also stand in contradiction with a tendency, underlined by Art. 12 GDPR, to prefer concise, transparent, clear, intelligible and plain language that avoids any legalism[6]. To try and take into account such transparency requirements, a favored approach consist of adopting a layered approach where a basic header will point out to a generic wording while enabling interested users to click on the full text[7]. Others mix visual (through videos) and textual elements[8]. Finally, privacy notices may also be tailored to specific needs, such as an icon that will notify data subjects of the presence of a CCTV for instance.

[Rz 21] As a result, a first step will consist of finding out whether your company already has such policies or notices in place and, in the affirmative, to revisit these documents in light of

5 See notably Art. 13-14 GDPR which require the following information to be disclosed at the time the data are obtained: (i) identity of the controller; (ii) contact details of the data protection officer, where applicable; (iii) purposes of the processing as well as the legal basis for such processing; (iv) description of the legitimate interests in cases where processing is based upon that basis; (v) the recipient or categories of recipients; (vi) where applicable, the transfer of collected data and applicable safeguards; (vii) the retention period; (viii) reference to data subject rights, including the right to withdraw the consent where consent is the basis for processing; (viii) the right to lodge a complaint and (ix) where applicable, the existence of automated decision-making. In cases where personal data have not been obtained from the data subject, the notice should also indicate the source from which the personal data originates.

6 See, among others: *Guidelines on Transparency under Regulation 2016/679 (wp260rev.01)* (Adopted on 29 November 2017, as last Revised and Adopted on 11 April 2018); CIPL, *Comments by the Center for Information Policy Leadership on the Article 29 Data Protection Working Party's «Guidelines on Transparency» adopted on 28 November 2017* (29 January 2018), at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_wp29_guidelines_on_transparency-c.pdf.

7 A good example of such an approach can be found at: https://privacy.microsoft.com/fr-fr/privacystatement.

8 https://www.nestle.com/aboutus/businessprinciples/privacy.

current requirements, bearing in mind that these may have to be translated to be intelligible to your customers should they reside in different markets and speak different languages. Any amendment to existing policies or adoption of new ones should also be communicated to existing customers through a defined process (for instance by email or through an online notice).

2. Lawful Basis for Processing

[Rz 22] The GDPR now puts more emphasis on the requirement to opt for a given basis to lawfully process data, as set out in Art. 13–14 GDPR.

[Rz 23] While consent has been heavily used in the past as a basis for data processing, privacy professionals tend to dis-recommend such basis as (i) any consent can always be withdrawn, thus rendering any further processing illegitimate and potentially putting business continuity at stake, and (ii) consent needs to be freely given which, notably in employment relations, is considered an undesirable basis to process employee data in most instances[9].

[Rz 24] Rather than consent, your entity may try and focus on the need to process any data based upon (i) performance of a contract (for instance in an employment relationship, or for a sales contract) or (ii) legitimate interests (for instance related to the data collected prior to entering into an agreement by candidates, or for direct marketing by mail).

[Rz 25] It might obviously be tempting for companies to use legitimate interest as a basis for most of their processing. One however needs to be cautious and should bear in mind to test its entitlement to use legitimate interests as a basis for processing through a legitimate interests assessment, by answering the following questions[10]:

- Is the processing necessary? Is there another way to achieve the desired outcome?
- Does the processing meet the reasonable expectation of the individual?
- Is the processing likely to interfere with the rights and freedoms of the individual?

[Rz 26] Ultimately, one may consider that legitimate interests may:

9 Countries such as Germany notably strongly oppose the use of consent in employment relationships.

10 The limited scope of this paper does not enable me to put these different bases under in-depth scrutiny at this stage. For further analysis on legitimate interests, see notably: CIPL, *CIPL Examples of Legitimate Interests Ground for Processing of Personal Data* (27 April 2017), at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_examples_of_legitimate_interest_grounds_for_processing_of_personal_data_16_march_2017.pdf; CIPL, *Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR* (19 May 2017), at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf. A good paper (that however requires registration, for free, to enable the downloading) related to the assessment of legitimate interests is: Data Protection Network (DPN), *DPN Legitimate Interests Guidance – GDPR (Version 2.0)*, at: https://www.dpnetwork.org.uk/dpn-legitimate-interests-guidance/. For further analysis on consent, see notably: *Guidelines on Consent under Regulation 2016/679 (wp259)* (Adopted on 28 November 2017); CIPL, *Comments by the Center for Information Privacy Leadership on the Article 29 Data Protection Working Party's «Guidelines on Consent» adopted on 28 November 2017* (29 January 2018), at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_wp29_guidelines_on_consent-c.pdf; CIPL, *CIPL White Paper on GDPR Implementation in Respect of Children's Data and Consent* (6 March 2018), at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_eprivacy_gdpr_fact_sheet_def_20_mar_18.pdf.

Definitely come into play	(i) fraud prevention, (ii) criminal acts, (iii) public safety or (iv) network/information security.
Probably yes	(i) use is reasonably expected, (ii) impact upon privacy is minimal, (iii) use is proportionate and (iv) provides a compelling benefit.
Maybe (assessment to be carried out)	(i) employee data, (ii) direct marketing (other than e-marketing) or (iii) client data.
Probably not	(i) use hard to anticipate, (ii) likely objectionable, (iii) likely harm to the rights and freedoms, (iv) reasonable alternatives at disposal, (v) excessive.

[Rz 27] For Swiss entities subject to the GDPR, it is worth remembering that, although using legitimate interests as a lawful basis may enable you to avoid the issue of consent withdrawal when such consent is the lawful basis for processing, data controllers will still have to face the entitlement of data subjects to object to such processing, as set out in Art. 21 GDPR. Unlike consent which, once withdrawn, mandates the processing to immediately be stopped, the right to object will however still enable data controllers to defend themselves and raise some defense to further process the data at stake.

[Rz 28] As a result of the emphasis put on the basis for processing, one will need to wonder while mapping its data the following:

- Do we have a suitable basis?
- Will we have to transition from one basis to another?
- Will there be a need to requalify all our processing based upon consent (for instance because we have no log related to such consent, or because our data subjects were not informed of the entitlement to withdraw their consent)?
- Can we collect, store and maintain evidence of consent?
- Are we able to store and maintain evidence of our legitimate interest assessment?

C. Vendor Management

[Rz 29] Vendor management will typically require you to: (i) assess your existing agreements and make sure that they comply with privacy requirements and (ii) make sure that future vendors meet their privacy obligations. This is a step where legal support, if not provided in-house, will be hard to avoid.

1. Agreements in Place

[Rz 30] A basis issue faced by all companies first consist of tracing and finding the existing agreements, a task that regularly proves daunting.

[Rz 31] If the number of agreements at stake is minimal, you may try and address them all; if you have hundreds, you will obviously have to prioritize after having carried out a risk assessment and identified the most critical agreements from a privacy standpoint (based upon different

criteria such as, for instance: categories and types of data at stake, their volume, purpose of the processing, location of the processing).

[Rz 32] Rather than reviewing each and every agreement, a more efficient way to process consist of drafting a data processing agreement (whose content will shortly be discussed below) that will be attached as a schedule to existing agreement, to supersede and replace any privacy provision in place.

[Rz 33] SMEs however have to be realistic; their – regularly – limited bargaining power will prevent them from being able to exercise much pressure on big players. As data controllers, SMEs however remain accountable to ensure that their vendors comply with their obligations; should it not be the case and should the vendors be unwilling to engage on your data processing agreement or have their own adequate privacy provisions in place, you will have no other choice but to take a business decision as a result of a risk assessment to decide whether to go on with that vendor or terminate the relation (which may well result in a dispute or prove difficult should all your fees have been prepaid) and look for an alternative supplier.

2. Future Agreements

[Rz 34] Privacy by design will require any data controller to assess their vendors and willingness to comply with privacy requirements, including, where applicable, as part of an RFP process. In practice, Art. 28 GDPR requires any form of data processing by a vendor to be contractualized. This agreement, that may be your data processing agreement, will typically have the following provisions in place:

- Subject matter and duration of the processing;
- Nature and purpose of the processing;
- Type of personal data;
- Categories of data subjects;
- Obligations and rights of data controllers;
- Data will only be processed on documented instructions from the controller (typically resulting from the agreement);
- Persons authorized to process have committed themselves to confidentiality;
- Adequate technical and organizational measures have been taken considering the data processed;
- Assistance to data controller with regards notably to data subject requests;
- Data return or deletion at the end of processing;
- Providing all information necessary to demonstrate compliance and allow for and contribute to audits.

[Rz 35] As part of your due diligence as data controller, you should also ensure that your vendor's employees are trained and have some privacy awareness.

[Rz 36] Ideally, you may also try and ensure that data will be processed (and notably stored on servers located) in EEA, although the recently enacted *Clarifying Lawful Overseas Use of Data Act* (so-called CLOUD Act, H.R. 4943) is likely to restrict the protection sought for[11].

[11] The text of the CLOUD Act is available at: https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

[Rz 37] Any data processing taking place outside of EEA by your vendor will indeed require specific safeguards. It is key to bear in mind that «processing» is not limited to the storage or modification of data as most businesses will tend to believe; «processing» is actually broadly construed, and merely accessing data remotely, for instance through an IT support provided from Bangalore in India, will be sufficient to amount to a form of processing taking place outside of EEA.

[Rz 38] In that case, you will need to ensure that you have an adequate transfer solution in place to allow such processing to take place. In practice, this will most of the time consist of the implementation of Standard Contractual Clauses (so-called Model Clauses), which also present the advantages of requiring information fairly similar to the ones requested in Art. 28 GDPR as part of their Annexes[12]. While US vendors will sometimes try and rather refer to the Swiss-U.S. Privacy Shield, most customers should try and avoid such reference, whose future still remains unclear (but whose validity is not at stake, yet)[13].

[Rz 39] Some vendors may also refer to their BCRs. BCR, if approved in accordance with Art. 47 GDPR, will enable the transfer between affiliates within the same group, including outside of EEA[14]. It is however worth remembering that the BCR will only enable the transfer of data intragroup, but will not justify the initial collection of such data outside of EEA, for which an adequate transfer solution such as Model Clause will still be required.

[Rz 40] Ultimately, data controllers should try and ensure that their vendors provide sufficient security safeguards, notably if they are cloud based, which can take the form of certifications such as ISO27001 or the delivery of a SOC2 Report (most commonly used ones), or that their service is hosted with a well-regarded cloud provider such as AWS or Azure.

[Rz 41] In my perspective, no matter your size, the most common issues faced when negotiating data processing agreements meant to align with GDPR requirements relate to the following provisions:

- *Subprocessors*: in theory, while processors may benefit from a general written authorization to engage subprocessors, they should inform the data controller of any intended change concerning the addition or replacement of other processors, so as to enable controllers to object to such changes. In practice, compliance with this requirement for cloud-based vendors is tricky; considering the multi-tenant environment their business model is built upon, they

12 See 2004/915/EC, Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (EU Controller to non-EU or EEA controller) and 2010/87/EC, Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries (EU Controller to non-EU or EEA processor), at: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en. Both clauses have been amended by the Commission implementing Decision (EU) 2016/2297 of 16 December 2016, at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016D2297.

13 https://www.privacyshield.gov/welcome.

14 *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules (wp256rev.01)* (Adopted on 28 November 2017 as last Revised and Adopted on 6 February 2018) as well as *Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules (wp257rev.01)* (Adopted on 28 November 2017 as last Revised and Adopted on 6 February 2018); CIPL, *Comments by the Center for Information Policy Leadership on the Article 29 Working Party Working Documents Setting up Tables for Binding Corporate Rules and Processor Binding Corporate Rules adopted on 29 November 2017* (17 January 2018), at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_wp29_bcr_working_documents_wp256_and_wp257_.pdf. A list of companies for which BCR cooperation procedure is closed can be found at: https://ec.europa.eu/newsroom/document.cfm?doc_id=40100.

cannot allow any customer to veto one of their sub-processors, so that any such objection will in practice result in the termination of the agreement subject to a potential refund of any pre-paid fees. Most vendors will however be reluctant to implement a process to even inform their customers of any change to their existing list of sub-processors and, at best, refer to a URL link that will be updated and that customers are expected to check from time to time. This obviously is far from complying with the information requirement set out in Art. 28(2) GDPR, but so it is.

- *Assistance*: while Art. 28 GDPR requires processors to assist controllers on several accounts (such as to address data subject requests or the execution of a data protection impact assessments), some vendors that are concerned about the potential costs resulting from such support will make a distinction between the provision of reasonable information (at no cost) and the further support that will be considered a professional service to be paid for, or will try and refer to a limited number of man days where their support may be requested at no cost.
- *Technical and organizational measures*: finally, some vendors will try and invite their customers to assess their technical and organizational measures so as to assess their adequacy with regards to the data to be processed, get their approval and, consequently, tentatively be exempt from any liability resulting from these measures deemed appropriate by their customers. In my view, this clearly is unacceptable, in the sense that vendors then try to shift the risk resulting from their own obligation to ensure that they have adequate technical and organization measures in place upon their customer, notwithstanding a clear separate and distinct obligation as processor to that effect in accordance with Art. 28 GDPR. It is up to vendors to make sure that they have the sufficient safeguards in place to comply with their obligation, rather than to get their customer's blessing to that effect.

D. Data Breach Response Plan

[Rz 42] Most SMEs are unlikely to be the primary target of data protection authorities' investigations. Such investigations may however be triggered as a result of a data breach. While data breach response plans are common in the United States of America, where each State has its own legislation on that regard, the obligations contained in Art. 33 GDPR are new on this side of the Atlantic. No matter whether your company is subject to the GDPR or not, the implementation of such a response plan sounds like a good practice in accordance with the accountability principle faced by any data controller. Contracting a cybersecurity insurance may also soon be part of the basics for any company and certainly appears to be a must at a time when the question of a data breach occurrence does not start with an «*if*», but rather «*when*».

[Rz 43] Without going into the details of what has been the subject of whole books[15], the implementation of a data breach lifecycle will typically consist of the following phases:

15 See, for instance: Liisa M. Thomas, *Thomas on Data Breach – A Practical Guide to Handling Data Breach Notifications Worldwide*, 2018. Focused more particulary on the GDPR, see: *Guidelines on Personal Data Breach Notification Obligations under Regulation 2016/679 (wp250rev.01)* (Adopted on 3 October 2017 as last Revised and Adopted on 6 February 2018); CIPL, *Comments by the Center for Information Policy Leadership on the Article 29 Working Party «Guidelines on Personal Data Breach Notification Obligations under Regulation 2016/679»* (1 December 2017), at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_to_wp29_guidelines_on_breach_notification.pdf.

- *Identification of the incident*: who reported the incident internally? To whom? When and at which location? How was the incident discovered? Who are the key stakeholders that should be included?
- *Evaluation of the incident:* before referring to a «breach», one should make sure that such a breach did actually tale place through primary investigations. What is the nature of the compromise? What type of information has been affected? What is their volume? What is the likelihood of the harm (for instance unlikely if all data were encrypted)? Do we need to hire external resources (such as a forensic company or a breach response remediation provider)?

  In case of an actual breach, your company will have three primary concerns: (i) to contain the incident and any affected system, (ii) have business back and running, and (iii) to assess whether notifications have to take place in accordance with applicable laws.
- *Reporting obligations*. One has to make a distinction between internal reporting within the company and notification obligations. No matter the type of communication, these have to be locked down so that inaccurate or incomplete information is not spread around your company or externally.

  Only the incident response team should be responsible for any such communication. The response team should consist of a minimal number of individuals to remain efficient, such as: legal counsel (internal, external), compliance (security, privacy), appropriate business unit whose data are at stake (finance, HR, marketing, etc.), IT and an executive decision maker.

  Question as to whether formal notification has to take place will have to be assessed by your legal counsel, who will have to answer the following questions: what are the applicable laws? Do we have a «breach» under these laws and what are the requirements? Do we have to notify and in what timeframe? To whom? Bear in mind that, should you have a cybersecurity insurance, your insurer is likely to play an important role and require regular communication.
- *Conducting notifications:* it is recommended to already have templates at disposal that might serve as a basis to notify relevant authorities and/or data subjects of the breach and to document and record all these notifications. Typical questions that may arise consist of finding out where affected individuals reside and whether you actually have all addresses required to notify (if need be).
- *Recordkeeping and debrief:* to record all steps and notifications taken will then enable you to track certain key performance indicators (KPI) such as, for instance: (i) how many notifications could be sent in a complete or partial format, (ii) what has been the average time to provide notice and (iii) how many missed deadlines or delays have you suffered.

  Once the breach is over, a debrief session with the privacy response team is recommended to learn the lessons from the past and answer questions such as: which parts of the process worked as intended? Which did not work at all? Why? Has any unforeseen difficulty been encountered? How much did the breach cost to the company?

E. Maintain Procedures for Inquiries and Complaints

[Rz 44] Privacy frameworks, as demonstrated by the GDPR, puts a strong emphasis on data subjects, not only through principles such as privacy by design and by default, but also through the granting of additional subject rights to put individuals in control on their data[16]: right of access, right to rectification, right to erasure, right to restriction of processing, right to data portability and right to object.

[Rz 45] The goal here is not to analyze each of these rights, but rather to ensure that companies have the relevant mechanisms in place to handle such requests (within a month when subject to the GDPR[17]), in answering the following type of questions:

- Is there a documented policy or procedure to address Data Subject Access Requests (DSAR)?
- Is your organization able to respond to DSARs within one month?
- Are there procedures in place to provide personal data to data subjects in a structured, commonly used, and machine-readable format? Data portability is, based upon my experience, one of the most difficult part for companies to comply with.
- Where applicable, are there mechanisms in place to allow personal data to be deleted or rectified?
- Are there mechanisms in place to stop the processing of personal data when a data subject seeks to restrict the processing?
- Are individuals informed about their right to object to certain types of processing?
- Are there mechanisms in place to stop the processing of personal data when individuals object to it?
- Are you able to deal with varying workloads?
- Are you able to check the data subject identity?

[Rz 46] While this set of questions is focused on GDPR, they may easily be transposed to SMEs that are not subject to the GDPR but will still have to face DSARs.

F. Training

[Rz 47] While security is key, data breach will in most instances be the result of negligence employees. In short, raising privacy awareness within your company is crucial and part of your accountability as data controller.

[Rz 48] Privacy training should therefore be conducted, both in general terms but also tailored to different units (such as HR or marketing for instance), and refreshed on a periodic basis[18]. Measuring attendance to these trainings as a KPI and making them mandatory might be a good practice as well.

[Rz 49] To maintain privacy awareness, the setting up of an internal data privacy portal, news and poster may also create over time a privacy mindset and culture within your company that should not be neglected.

16 See Art. 15–21 GDPR.

17 Art. 12 GDPR.

18 For an example of a basic training provided for free in French and supported by the Fédération des entrepreneurs romands, see: http://medias.fer-ge.ch/FER/rgpd/#/?_k=nk7525.

[Rz 50] Finally, depending upon the significance of your processing, having a member of your team attend conferences, seminars, webinars or even get certified may prove valuable[19].

G. Need for a Data Protection Officer?

[Rz 51] The requirement for a Swiss SME to appoint a data protection officer within the meaning of Art. 37 GDPR will be rare. Such will only be the case if your company's core activities require regular and systematic monitoring of data subjects (residing in EU) on a large scale[20]. Typically, this may happen if you run an e-commerce website targeted towards EU residents (because you have a local version registered under the ccTLD of an EU country, and/or because of the currency used on your website).

[Rz 52] Ultimately, this should be the exception rather than the rule[21]. From a governance standpoint, it will however be important to have someone in charge of ensuring that your privacy obligations are met and that will act as a contact person for privacy related matters. Ideally, it always is easier to have someone in charge internally, as such person will know your company and processes, but an outside counsel, typically a law firm, may come into play if you consider such external hiring more efficient. Depending upon the size of your company, involvement of cross functions such as IS/IT, HR or Marketing may also come into play through the appointment, for instance, of a privacy champion that will be the liaison point within the unit for privacy related questions after having been trained himself, thus creating a privacy team within your company.

III. Conclusion

[Rz 53] As highlighted in this paper, setting up a privacy management program can be achieved through basic steps which, although cost and time consuming to some extent, remain achievable even if you are not a privacy expert, in particular considering the numerous digital resources now available.

[Rz 54] While the methodology may obviously depend, typical steps will include:

- *Data Mapping*, with the objective to understand the type of data you process, by whom, from where. The mapping will be the starting point for your due diligence exercise and may serve as a basis for any future inventory.

19 The IAPP for instance provides several types of certification programs, see: https://iapp.org/certify/.

20 See: *Guidelines on Data Protection Officers (wp243rev.01)* (Adopted on 13 December 2016 as last Revised and Adopted on 5 April 2017); CIPL, *The Role of the Data Protection Office (DPO) and Risk and High Risk under GDPR* (5 October 2016), at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_workshop_ii_report.pdf; CIPL, *Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation* (16 November 2017), at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_gdpr_dpo_paper_17_november_2016.pdf.

21 One however needs to remember that the fact for a Swiss company to be subject to the GDPR may require the appointment of a representative in the Union unless such processing of EU residents is occasional, does not involve special categories of data, criminal convictions or offenses and is unlikely to result in a risk for the rights and freedoms of individuals (Art. 27 GDPR). Having such a representative seems to be a difficult task, as such representative may then endorse liability, which few entities are obviously willing to take. On that regard, having a law firm appointed might be a good alternative, although likely to come at a price for the risk then taken.

- *Privacy policies and notices.* To draft from scratch or review your existing policies is likely to be the next step, notably to take into account current practices and requirements, which may lead you to reassess your basis to ensure lawful processing and document such basis accordingly.
- *Vendor management*. Largely ignored, vendor management will require you to make sure as a data controller that your vendors comply with their obligations in accordance with applicable data protection laws by having a relevant set of provisions in place. This ideally should not only relate to vendors with whom you may engage in the future, but also with existing ones. Having a data processing agreement template in place that can be attached to vendor agreements as a schedule might be a good starting point.
- *Data Breach Response Plan*. Incidents are likely to be the triggering event raising authorities' attention for SMEs. As a result, it is key to have a proper response plan in place and know the resources (notably external ones) that you may have to promptly contact should any such breach occur. Typical steps will consist of: (i) identify the incident; (ii) evaluate the incident; (iii) report obligations; (iv) conduct notifications and (v) record keeping and debrief.
- *Maintain Procedures for Inquiries and Complaints*. Legislators, as in the GDPR, consider it key to enable individuals to control their data. To that effect, individuals increasingly benefit from different rights that will require an internal assessment to make sure that you have the proper resources, mechanisms and processes in place to comply with such obligations.
- *Training*. Having a privacy management program on paper without bringing it to the attention of your team makes little sense. Training is considered a key concept of privacy by design within a company, and general as well as tailored training to be delivered to the different units, ideally mandatorily and refreshed on a period basis, thus become a must to demonstrate your accountability.
- *Data Protection Officer.* Last but not least, if will be important to assess whether, considering the mapping carried out and your business model, the appointment of a data protection officer is needed as set out under Art. 37 GDPR. Such should rarely be the case for Swiss SMEs. Notwithstanding the absence of a mandatory appointment of a data protection officer, having someone acting both internally and externally as a point of contact for any privacy related matters to ensure compliance on an ongoing basis and address data subject requests will be important.

Philippe Gilliéron, Attorney at Law (TIMES Attorneys), Professor at Lausanne Law School.