WilhelmGilliéron
AVOCATS

Auteur: Wilhelm Gilliéron Avocats | Le : 3 May 2021

The new Federal Law on Data Protection: take some actionable steps, yes! Panic, no!

"*What are you doing with my data? "Why are you asking me for my phone number? "Do I have to fill in your customer form? Do I have to give you all this information?* ". All these questions, which many merchants have to face today, were not asked a few years ago.

In the digital age, data protection has been put into light, a light reinforced by the media's interest in reporting the slightest incident. The acceleration of digitalization as a result of the pandemic has only reinforced this attention.

Although often described as a "*gas factory*", one cannot deny that data protection plays a fundamental protective role in the fight against the ever-increasing asymmetry of information between suppliers and individuals, a disparity that is obvious when one considers the predominant role played by Big Tech.

At a time when a new Federal Law on Data Protection has just been adopted and that the Federal Council is working on draft ordinances to come into force by the end of 2022 or the beginning of 2023, the question arises as to what steps should be taken to demonstrate that your company is aware of the significance gained by data protection and that you do care about your customers'data.

In reality, there is no need to turn this into a "*gas factory*", as the measures to be taken depend largely on an assessment of the level of risk with regard to the data processed, their categories, volumes, purposes, etc.

In the vast majority of cases, the following six measures, which can be taken at a reasonable cost, will be sufficient to ensure compliance

1. Inventory of personal data

The establishment of an inventory consists of listing the different types of data processing that the company performs. Although such an inventory will not be mandatory for many companies that do not reach a critical size, its establishment appears to be a best practice that will make it possible to become aware internally of the processing carried out and to raise the awareness of management and employees in the field of data protection. Taking the necessary time to map your data processing is therefore far from being a waste of time.

The types of processing carried out can be more or less numerous. For the vast majority of SMEs, they will typically concern two main categories of individuals: employees on the one hand (payment of salaries and social contributions, processing of sick leave, vacations, interviews, etc.) and customers on the other hand (placing of orders, after-sales service, marketing).

For each type of processing, the company will identify its subcontractors, which are becoming increasingly numerous in the field of IT (for example Microsoft in the case of recourse to a cloud platform such as Azure or O365, or SAP in the field of human resources, to take just two examples) and the possible transfer of data abroad. Setting up the inventory will be an opportunity to question the existing service providers, to assess whether proper agreements are in place (including data protection and security clauses) as well as the retention period of these data, which is often completely ignored.

For smaller companies that want to make such an inventory, this task can be performed by one person. For larger companies, it should be delegated to unit managers, who are in direct contact with the data processing at stake. If this task is to be performed internally, my experience is that support and review by a legal expert is not useless, as internal teams often have a hard time identifying all the providers that process their data, especially in IT.

The document is not static, but dynamic and evolving. It should therefore be completed as and when new processes are carried out.

The authorities often provide useful documents to help establish the inventory and ask the right questions; this is particularly true of the CNIL in France.

2. Privacy policy and other contractual documents

In order to show a clean slate, the establishment of certain contractual documents appears to be essential, without requiring much effort. A distinction can be made here between internal and external documents.

Internally, it is useful to have a privacy policy (usually mentioned on the website along with a cookie notice), which defines in a general way the type of data collected and the processing performed. It is also now common practice to establish a directive concerning the processing of employee data.

Externally, a standard data processing agreement should be drawn up to ensure that external providers meet a certain level of requirements. While many providers will now have their own data processing agreement, having a standard document will help ensure that the provider's agreement meets the company's requirements and, where appropriate, will be provided to the provider if it does not have one.

3. Privacy Impact Assessment (PIA)

If a proposed data processing operation is likely to present a high risk to the individual (e.g. large-scale processing of medical data), then what the law calls an impact assessment must be carried out. The purpose of a PIA consists of assessing the level of risk of the processing, even if it means obtaining the prior approval of the Commissioner. In this case, the multidisciplinary exercise will most often require the use of a lawyer who can provide expertise in the field.

For the vast majority of SMEs, however, such an exercise should remain limited, with the exception of certain specific fields such as health.

4. Process for the exercise of the rights vested in individuals

With the coming into force of the new federal law, the rights of individuals will be extended. In essence, any company will have to be able to tell any individual who wants to know whether it is processing data about him or her and, if so, which data.

It is then useful to ensure that such data can be easily detected, which should be the case for small SMEs, but can sometimes be more difficult when individuals' data are processed at different levels by different actors. The inventory will then be a useful tool to locate these data in view of the processing performed.

The establishment of standard processes and response templates can then be useful to facilitate and systematize the processing of such requests in a uniform and consistent manner.

5. Establishing a security incident response plan

Since any security incident today can have a significant reputational impact not to say operational, it is fundamental to ensure that the data being processed is surrounded by adequate security safeguards given the level of risk.

Either the company in question subcontracts the management of its IT infrastructure to a third party, and it is then responsible for ensuring that, contractually, the provider in question has provided the necessary security guarantees (e.g. by having certain certifications, or that the data center used is in Switzerland or at least in Europe, or that a disaster recovery plan is in place, etc.); or the company manages its own IT infrastructure, and it must then ensure that the level of security surrounding the processing of data is sufficient.

It is often considered today that the question to be asked is not whether a security incident is likely to occur, but when. This raises many questions: How to react? Who should react? What should be done first? Should I close the accounts, isolate the system? Who should be informed? Should employees, authorities or the public be informed? Formalizing the process to be followed in the event of such an incident is therefore a sign of caution and, once again, of awareness enjoyed by the company as to the importance of protecting data.

6. Training

Finally, it is useful to make employees aware that the company considers data protection as part of its business processes, by providing them with training, which can be uniform or, if necessary, specified according to the position held by the employee (e.g. receptionist, human resources, marketing, etc.). Experience has taught me that basic training can easily be provided in 1 to 1.5 hours, a reasonable amount of time to make each employee accountable.

7. Conclusion

Ignorance is often a source of rejection. Data protection is no exception. Unknown, it is often rejected for fear of the efforts and budgets that most SMEs believe must be devoted to it. However, a few simple measures at reasonable costs are enough to achieve an acceptable level of compliance for the vast majority of SMEs, whose processing is often limited and whose risks are easily contained.

Source : https://www.wg-avocats.ch/en/news/data-protection/new-federal-law-data-protection/