Entrepreneurs, GDPR is not your nightmare!

By Anne Tschanz Vakula – published in french in AGEFI –www.agefi.com - April 24, 2018
http://www.agefi.com/quotidien-agefi/une/detail/edition/2018-04-24/article/la-chronique-danne-tschanz-vakula-474483.html

First of all, before being entrepreneurs or bosses, you are human beings. You want your personal data protected. If you have selected "Friends Only" in your Facebook profile for the photos and messages you post, you do not want people other than only your "Friends" to have access to them, and if this condition was not met, if your trust was betrayed, you would like to have the right to take the case to court and get compensation. Well, the European General Data Protection Regulation (GDPR) [(EU) 2016/679], which becomes enforceable May 25, 2018, is based on the same idea!

As an entrepreneur, your nightmare would be to wake up one morning with the list of your customers and the different profiling done by the marketing department of your company published on internet, for example from a server in Ukraine, without any way to be able to do anything: hackers did not even bother to ask for ransom before publishing ... were they paid by a competitor? Your nightmare would be to wake up one morning and receive a summons to such a German court following the complaint filed by one of your customers domiciled in Frankfurt who would have received by mistake a message that one of your employees based in Lausanne sent to another of your employees based in St. Gallen. Bad luck, this email contained sensitive information about a group of customers and a targeted marketing project.

The GDPR does not prohibit the collection, processing, analysis, profiling, use, and storage of customer and employee data. But it imposes very serious shields. It creates a framework, specifies ways and means, and obliges to adopt an adequate organization.

It is not just a matter of updating contracts, the so-called "terms and conditions" of 267 pages and other "disclaimers" longer than Stephen King's *The Stand*, and asking your IT specialist to raise the level of security of your systems.This is a complete revolution in the matter of working with data. The "all digital" has increased dramatically the risk of loss, leakage, theft, misuse or malicious manipulation of data. Every employee in the company must feel comfortable with the data they handle in relation to the GDPR.
It is not just a question of compliance with the law, it is also a question of respect of the trust your clients place in you.

It is unreasonable to wait for the adoption of the revised version of the Swiss Law on Private Data (LPD). Indeed, the probability that your company located in Switzerland is subject to the GDP is high. The submission criteria have nothing to do with whether or not you have something to do with social networks, like Facebook.

A Swiss company can be challenged by one of its customers residing in Spain, or by one of one of its employees, residing in neighboring France, who uses a corporate cell phone to respond to customers during evenings or weekends, when this employee finds himself on French territory ...

The Geneva Compliance Group (GCG) has created an excellent questionnaire (https://genevacompliance.com/en/GDPR.html) in order to quickly obtain a free check. The company Lexing (https://lexing.ch/rgdp/) or the FER kit (https://www.fer-ge.ch/web/fer-ge/-/kit-rgpd) allow you also to obtain valuable information and advice.

GDPR compliance is far from being a nightmare, but is rather an opportunity: the process of analyzing relevant customer data will certainly enable you to evolve your business in depth, to inject some new and innovative, more profitable strategies into it, to develop new customer segments and even generate additional revenue!

Finally, like all of you, I was both **stunned and stupefied** by Cambridge Analytica (CA) "legally siphoning" data of 80 million US Facebook users. If the mission and responsibility of the members of a board of directors is not, among other things, to monitor, and where appropriate, to denounce and stop sources of revenue that are obviously the result of a subterfuge (CA claimed that the questionnaire, which was sent in advance to advertising messages aimed at elections, had as goal purely academic research) and other abusive exploitation of the business model of the company, then what are the board members for? And in your company, has an analysis of the risks induced by each contract in terms of data protection been conducted?

Do not wait to be summoned in front of a Congress Commission... or a European court: put your company in conformity with the GDPR!