FRANCE CREANCES
Credit management & debt collection services since 1970

Toulouse, France, October, 3rd, 2019

WHY SHALL WE NOT IGNORE THE GDPR COMPLIANCE?

Dear colleagues of LIC, dear friends,

For those of you who were attending our last LIC conference in Athens, you may remember that we spoke about GDPR. Please find below a short note to help those of you who are not yet too familiar with this complex European law and its consequences on our businesses.

What is GDPR in short ?

GDPR is the General Data Protection Rule that is in force across the European Union since May, 25th 2018. Since then, all firms across the EU i.e. all the legal entities registered in on of the EU countries, shall be already 100% compliant with GDPR; whether these firms are big or small, from the private or public sector. IN clear, we are all supposed to be already 100% compliant.

What is considered as personal data ?

Personal data definition is very wide; examples are : names, postal address, email address (including business ones), phone numbers (including business ones), medical data, political opinions, religious beliefs', banking data, employment data, …etc. in other terms this means all information that gives indication about who we are, what we do, what we think… ; knowing that data can be stored on physical documents, USB keys, IT servers, email inbox, social network accounts, extranet accounts…etc., in full or in part, all measures taken shall be adapted to all possible supports as well.

What are the risks vis a vis personal data breach ?

GDPR does not only make private or public organizations responsible for taking all appropriate measures so as to protect personal data against all physical or cyber security breaches; GDPR also makes these organizations liable in case of personal data breach.

What if an organization is not GDPR compliant ?

Under GDPR, the fines from each national Data Protection Agencies can be very severe against companies that are not compliant : up to €20m or 4% of the global turnover. This is very significant. All organizations are concerned. This cannot be simply ignored.

What shall be done to comply with GDPR ?

GDPR compliance takes a lot of time & efforts; all employees or members of an organization are concerned. We can identify 6 main steps to get towards GDPR compliance; below is only the summary.

Step 1: Nominate your DPO (Data Protection Officer) to lead the data governance inside your organization. Your DPO will have 3 main missions: inform, advise and control. Your DPO shall be neutral in all circumstances so DPO shall preferably not be the boss or the owner of the organization; the DPO can be external from your organization, if competent. DPO shall be trained as well as all your teams.

Step 2: Map all your processes that deal with personal data in your organization. All these processes shall then after be listed & documented in a dedicated registry.

Step 3: Prioritize all the actions to be taken based on the risks identified from the registry of the various personal data processes.

Step 4: Manage your risks that could generate a breach of personal data (i.e. when inappropriate data is collected or is retained for too long, or collected although it is not absolutely needed, or could be stolen from outside/hacked from your servers). Personal data impact assessment shall be run for each one of these risks.

Step 5: Organize your internal processes so as to ensure a high level of permanent protection of data against all possible events that can happen (physical security breach; IT security breach; management of the rights of people whose data are used by your organization; change of vendor…).

Step 6: Document your compliance. GDPR documents and processes shall all be stored in one place, regularly updated and continuously checked.

FENCA board and members (including myself) have been working hard over the past 3 years to issue a Debt collection industry GDPR specific Code of Conduct. If approved, this Code of Conduct would help our debt collection companies to comply with GDPR a bit more easily. This Code of Conduct should be approved by the European Data Protection Board soon; it's a must before it can be enforced. We hope to get this done within the few next months.

I'm not a GDPR expert, but please get in touch if you think that I can help you. I will do my best.

Kind regards,
Christophe

Christophe NOBILET
GCE-FRANCE CREANCES
Owner & CEO
c.nobilet@france-creances.com
+33582951618
+33650934984