Regulation and Competition

How to Build a Customer/Prospect Database Lawfully in France

Chloé TORRES & Emeline BISSONI
Alain Bensoussan law firm, Paris

Customer/prospect data are essential to life and business and are sometimes part of the company's assets. Some companies are even putting data at the core of their business model by offering list rental, database development, behavioral segmentation services, etc. Coupled with "Big data" (FORGERON, 2012) (exponential growth of data generated) - a now unavoidable phenomenon for companies data will become the new raw material of companies according to economists (HUMBERT, 2012).

To enhance the data it holds, uses or otherwise collects on the internet, a company must master not only technical aspects but also legal aspects and in particular personal data law. As a matter of fact, data will have value only if the company uses it in compliance with the applicable regulation and with full openness towards consumers. A way to achieve this is to implement a data privacy policy, as it clearly offers companies a competitive advantage and boosts the trust of current or potential customers.

Lawmaker has long since adapted the existing legal rules to provide a basis for the building and use of databases and reduce the risk of violations of individual freedom for fear of "Big Brother". Today, the European lawmaker is going one step further by planning to integrate the notion of "privacy" at the earliest possible stage of the design process of databases: the European Commission indeed plans to make mandatory the "Privacy by Design" (PbD) approach in the proposed EU Regulation to replace Directive 95/46/EC on the protection of personal data (TORRES, 2012).

This paper will address the growing need to consider law in the development of customer and prospect databases and show that law can be a tool for value-building and risk management.

Legally-obtained data is value-added data

Businesses must comply with certain obligations when using personal data (obtained from customers, suppliers, prospects, consumers, …). In the European Union, the legal framework concerning the protection of this kind of data is the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1]. This directive has been transposed in all the European Union countries through different data protection acts but the fundamental principles and obligations are almost the same in all countries.

As an example, in France, companies that want to build and operate a client/prospect database must essentially comply with two texts: the French Data Protection Act [2] and the French Act for Confidence in Digital Economy, a.k.a. "LCEN" [3].

The French data protection act in brief

The French Data Protection Act imposes several obligations, and we will only discuss here those concerning customer and prospect databases. The main obligation is to notify the customer and/or prospect database to the French data protection authority, the CNIL, or include it in the list of the processing kept by the company's data protection officer, as the case may be.

The data controller must also provide the individuals from whom the data are collected (customers, prospects, visitors, etc.) with relevant information,

---

1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

2 Act no. 78-17 of January 6 1978 on Information Technology, Data Files And Civil Liberties (*Loi 78-17 du 6-01-1978 relative à l'informatique, aux fichiers et aux libertés*).

3 Act no. 2004-575 for Confidence in Digital Economy (*Loi n° 2004-575 du 21-06- 2004 pour la confiance dans l'économie numérique*)

such as, in particular, their right to access the data about them, object to their listing in a database, request that their data be updated, etc.

He must also make sure that the individuals from whom data are collected can object, without cost, to the use of their data for direct marketing purposes. Thus, he cannot resell the data if the persons to whom they belong have not been notified beforehand.

Moreover, the data controller must regulate the possible transfers of customer/prospect data to countries outside the European Union, for example if those are required for the hosting of the data on a cloud computing system, for an email routing agreement with a service provider, etc. But companies should be careful: while on-demand cloud services provide an easy-to-use and cost-effective way to host data, in most cases the client does not pay attention to where his data are located. No matter how simple cloud services can be, businesses should not forget that IT systems are complex and that the protection and security of personal data should be ensured at all times.

The French Data Protection Act in fact requires the data controller to take all useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorized third parties.

The threats to personal database systems are numerous: disclosure of confidential information, falsification, accidental loss of personal data, etc.

Security has to be designed for all the processes concerning such data, whether it relates to their creation, their use, their backup, their safeguard or their destruction and includes their confidentiality, their integrity, their authenticity and their availability.

Companies must absolutely guarantee the security of the data; otherwise they will face criminal sanctions. Data security is increasingly burdensome. As data are becoming more numerous, they are increasingly difficult to secure: the bigger the data, the bigger the responsibility.

Failure to comply with the above obligations can have financial and brand image impacts. Most offences can lead to 5 years' imprisonment and a fine of €300,000. The CNIL may carry out an inspection and impose sanctions if violations of the French Data Protection Act are found.

Companies should indeed be careful as the CNIL has dramatically increased the number of its inspections (more than 300 in 2011) and regularly receives claims from consumers for breach of their rights to be deleted from a customer database and no longer receive advertising e-mails (about 5,000 complaints received in 2011). Inspection and claims are a major risk for companies as they can result in a public warning published by the CNIL, which may be highly detrimental for the reputation and brand image of a company; and this may lead to a loss of trust not only from consumers, but also from partners and clients.

To help data controllers meet their obligations regarding the security of the personal data they collect, use and maintain, the CNIL has published a Guide on Personal Data Security (English translation available online) (*Guide Security of Personal Data*, 2010). This document comprises various fact sheets focused on a specific data security issue (e.g. authentication; maintenance; archiving; anonymization; encryption, …). Each fact sheet includes an overview of the issue, security do's and don'ts, as well as guidelines and recommendations for improvement. With the useful checklist attached at the end of the document, data controllers can assess the level of the security measures already in place in their organization and identify which measures should be taken to improve the protection of personal data.

The LCEN in brief

Article 22 of the French Act for Confidence in Digital Economy of June 21, 2004 (LCEN), lists the conditions in which companies can conduct direct marketing operations. Under the LCEN, direct marketing operations consist of "any message intended to promote, directly or indirectly, the goods, services or image of a person selling goods or providing services".

The said Article 22 prohibits the sending of any direct marketing message to an individual without having obtained his or her prior consent "Direct marketing by means of automatic calling machines, fax machines or electronic mail, in any form, using the contact details of a natural person who has not given prior consent to receive direct marketing in this way, is prohibited".

Consent must be free, specific and informed. In practice, it may be given for example by ticking a box on a data collection form.

Article 22(2) of LCEN defines "consent" as "any manifestation of free, specific and informed will whereby a person accepts that personal data concerning them may be used for the purposes of direct marketing".

Article 22 further provides that individuals must be offered the possibility to refuse, free of charge - other than charges related to sending the refusal - and in a simple manner, that their contact details to be used when they are collected and every time an email is sent to them for direct marketing purposes.

Each direct marketing message must also indicate valid contact details to which the recipient can send a request to stop receiving these messages free of charge, other than charges related to sending this request. It shall also indicate the identity of the person on behalf of whom the message is sent and the email subject line must mention an item related to the service offered.

A company should therefore implement a process allowing to obtain the prior consent of the customer and/or prospect targeted by the direct marketing campaign. If the company uses a third party provider to carry out the direct marketing operations (e.g. list rental, e-mailing), it should make sure that the said third party will provide for an opt-in procedure.

Concretely, the direct marketing email sent by the company to the customer must contain the following information:

- the possibility for the customers to object, free of charge - other than charges related to sending the refusal - to the use of their contact details;
- valid contact details to which the recipient can send a request to stop receiving these messages;
- the identity of the person on behalf of whom the message is sent;
- an email subject line related to the service offered.

The LCEN provides a derogation from the principle of prior consent where the individual has already been contacted for a sale or the provision of a service for "similar" goods or services by the same company. Consequently, if one of the partners of the company wishes to send commercial messages to promote "similar" goods or services, it may do so without first obtaining the prior consent to the individual.

Failure to obtain a prior consent is punished by a €750 fine for each message sent illegally.

In view of the many statutory obligations imposed on companies and the related risks, companies are strongly advised to implement a data privacy policy adapted to their line of business in order to reassure both its consumers and business partners.

"Pivacy by design " (PBD) is a risk-management tool

Any new technology brings about new risks. The potential intrusiveness of some of them requires that privacy and personal data protection be taken into account and protected from the outset: this is the "Privacy by Design" (PbD) approach advocated by the European Commission through the regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data dated January 25, 2012. The PbD approach may be further strengthened by the appointment of a company's data privacy officer.

The privacy by design approach

The Privacy by Design principle means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal. This in particular means that the protection of data must be at the heart of a company's internal processes.

Adopting a PbD approach is a very visible trend in international groups and such a trend is expected to grow by leaps and bounds in the B-to-C industry. Privacy by Design can serve as a new tool to stand out from competitors and be a further mark of quality and trust for clients and consumers. It will become pervasive, to the extent that it is in line with the spirit of the draft EU General Data Protection Regulation that is expected to amend Data Protection Directive 95/46/EC. The European Commission is indeed planning to make the Privacy by Design approach compulsory and proposes to adopt Privacy by Design for all products, services and systems involving personal data.

According to consultants, "it does not matter whether technology is initially invasive, since it can subsequently be corrected and accompanied by devices improving or adjusting the processing of personal data according to the purposes of device" (GBH-Consultant, 2012). This is what some call "transformative technology" (CAVOUKIAN, 2009).

For French MP Patrick Bloche - who presented a report on a motion for resolution related to data protection in February 2012 - PbD should be encouraged to give Europe "a genuine industrial digital policy and enable it to benefit from an undeniable comparative advantage in global competition" (French National Assembly, 2012).

With a Privacy by Design policy, companies can make sure that the processing of personal data they are carrying out is consistent with the data protection legislation; it is therefore a tool for legal risk management.

The first step in setting up a Privacy by Design policy is to work out a methodology that will reflect it in technological projects. Next, an in-depth analysis of the processing concerned needs to be conducted. Based on the findings of the analysis, the company will be able to draft specifications, to be used for the building of the database, containing accurate features of the customer/prospects database. In this way, it will be easy to put the processing in line with the provisions of the applicable law. In addition, the company will have complete visibility on the categories of data, the origin of the data and the retention period of the data.

This allows to achieve fully transparency and satisfy consumers who want to obtain information on the processing of their data. A data privacy policy will be even more effective if completed by the appointment of a DPO.

The appointment of a company's data privacy officer

The role of a Data Privacy Officer (DPO) is to ensure that the company complies with the various obligations laid down in the data protection legislation. The DPO is the company's focal point for data privacy and related issues. Since its creation in 2004, nearly 8,000 companies in France have chosen to appoint a DPO (in French Correspondant informatique et libertés, also referred to as "CIL").

Appointing a DPO is not compulsory in France; however, it should be emphasized that, as currently, drafted, the draft General Data Protection Regulation published by the European Commission on January 25, 2012, will make the appointment of a DPO compulsory where the processing is carried out by a company employing 250 persons or more and require regular and systematic monitoring of data subjects and present specific risks with respect to the rights and freedoms of data subjects.

Appointing a DPO has many advantages. First of all it enhances legal certainty. Failure to comply with the French Data protection Act can cost a lot to infringers, especially since the 2004 reform (French National Assembly, 2012) that increased the amount of the fines and extended the powers of control and sanction of the CNIL. Designating a DPO allows a company to reduce legal risks as the DPO:

- promotes full and ongoing compliance with the legal rules by acting as a one-stop shop for all data privacy issues; the DPO works hand-in-hand with the management and becomes the go-to person for data privacy and related issues;
- makes sure that the company's IT resources develop without jeopardizing the rights of customers and employees in their data;
- provides a regular legal watch, keeping the company abreast of up-to-the-minute changes and news in data privacy law;
- eases the successful application of the Act No. 2004-801 of August 6, 2004 that amended the Data Protection Act.

Secondly, it enhances the image of the company with consumers and business partners. The designation of a DPO showcases the company's commitment to comply with the data protection legislation and the recommendations expressed by the data protection authority. It also gives a competitive edge to the company, as it is a way to enhance competition by increasing the degree of trust of employees and customers towards the company.

It also contributes to a quality approach. A company can leverage the skills and duties of the DPO (e.g. the DPO has to draft and keep up-to-date a list of all the processing operations carried out in the company) to pave the way for and/or enhance a data management quality approach across the company, with a special focus on the processing of personal data.

Finally, with a DPO, a company is better able to strike the right balance and dovetail the day-to-day realities of the company into the legal framework (statutory requirements and recommendations of the data protection authority), while keeping up with the fast-changing, ever-evolving data-demanding technologies.

In an era of globalization, the database industry is faced with new challenges related to personal data protection and privacy, intensified by the "Big data" phenomenon, Companies can use law as a tool for meeting these challenges.

References

Act 2004-801 of August 6, 2004, amending Act No. 78-17 of January 6 1978 (*Loi 2004-801 du 6-8-2004 modifiant la loi 78-17 du 6-1-1978*)

CAVOUKIAN A. (2009): *Get Smart About Privacy: Smart Privacy and Privacy by Design*, October 20 2009.
http://www.ipc.on.ca/images/Resources/2009-10-20-IAPPKnowledgeNet.pdf

FORGERON J.-F. (2012): "Vous avez dit Big Data ?", Blog tendance "Informatique et droit", 3 May.
http://www.alain-bensoussan.com/avocats/vous-avez-dit-big-data/2012/05/03

French National Assembly (2012): report no. 4326, 7 February.
http://www.assemblee-nationale.fr/13/pdf/rapports/r4326.pdf

GBH-Consultant (2012): "Une place au droit dans la Privacy by design ?", Chronique juridique du 1er mars 2012. http://www.gbh-consultant.fr/?p=44

Guide Security of Personal Data (2010):
http://www.cnil.fr/fileadmin/documents/en/Guide_Security_of_Personal_Data-2010.pdf

HUMBERT F. (2012): "Big data : la nouvelle matière première de l'entreprise, à côté du capital et du travail", *Le Nouvel économiste* n° 1600, 16-22 February p. 67.
http://www.lenouveleconomiste.fr/lesdossiers/it-big-data-13734/

TORRES C. (2012): "Privacy by design", Blog tendances "Informatique et libertés", 11 May.
http://www.alain-bensoussan.com/avocats/category/blog-tendances/informatique-libertes-blog-tendances