Protecting Personal Data: Companies Not in Compliance With EU Regulations Face Serious Penalties

By François Berbinau

On May 25, 2018, regulation n°2016/679, called "General Data Protection Regulation" (the "Regulation"), issued by the European Parliament and the Council of the European Union (EU) on April 27, 2016, became effective. And it appears that a large number of companies will not have taken the necessary steps to be in compliance despite the very severe penalties involved.

In the current digital world, any company, regardless of its size or business sector, is regarded as a controller of personal data processing. Therefore, each company must comply with the new European data privacy legal framework and constantly maintain such compliance under penalty of sanctions which could put it at risk.

1. The Company: A Controller of Data Processing

According to the Regulation, personal data means "any information relating to an identified or identifiable individual."[1]

To ensure the same protection of personal data all over the EU, the Regulation provides a strict frame of data processing.

Personal data processing means "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means.*"[2]

Hence, this definition refers to the following operations on personal data:

- procurement;
- storage;
- modification;
- reading;
- use;
- transfer;
- cross-referencing ;
- removal.

In fact, any company whose clients are individuals has information on them such as their names, contact details, purchase history, reports from the customer service, list of outstanding invoices, etc.

Moreover, any company with employees gathers information such as curriculum vitae, cover letters, contact details, social security numbers, banking information, diplomas, recordings of video surveillance, pay slips, professional assessments, disciplinary records, dismissal letters, etc.

François Berbinau

In addition, when implementing a contract executed by two companies, one or both of them may obtain various pieces of information regarding several individuals, such as employees of its co-contracting party.

Thus, all of this processing of personal data relating to European citizens will have to be compliant with the new Regulation, which guarantees the protection of these data subjects.

2. A New Unified Legal Framework Applicable in All EU Member States

This new legal environment includes two distinct sets of rules: the general rules applicable to all personal data processing (2.1.) and the specific rules in case these data are transferred to an international organization or a country outside of the EU (2.2.).

2.1. General Rules Applicable to Any Personal Data Processing

The Regulation unifies the legal framework across the EU and establishes a common set of principles relating to the processing of personal data.[3]

According to the Regulation, personal data that are collected must:

- Be lawful, fair and transparent;
- Have explicit and legitimate purposes;
- Be adequate, relevant and limited to what is necessary;
- Be accurate and kept up to date;
- Be kept in a form which permits identification of data subjects;
- Be kept for a limited term according to purposes;
- Enjoy an appropriate security.

Compliance with all these principles has to be guaranteed by the controller of data processing, who must be able to produce proof of such compliance.

In order to ensure that these guarantees will be duly respected, the European legislator has issued a significant number of obligations that each company is expected to meet.

"Penalties provided in case of non-compliance with the Regulation are of three kinds: administrative (3.1.), civil (3.2.), and criminal (3.3.), and these are cumulative."

Hence, to ensure that its contemplated processing of data is lawful before it starts implementing it, the company must:[4]

- Verify that such processing is necessary for the performance of a contract, or in order to comply with a legal obligation, protect the vital interests of the data subject, or perform a task carried out in the public interest;
- Obtain the unambiguous consent of the data subject.[5]

During and after the processing of data, the Regulation grants the data subject a series of rights: a right of access,[6] a right to rectification,[7] a right to be forgotten,[8] a right to the restriction of processing,[9] a right to data portability,[10] and a right to object.[11]

To guarantee these rights, the company[12] and its controller's representative are also subject to the following obligations:

- Guaranteeing data protection by design and by default;[13]
- Keeping a record of processing activities;[14]
- Actively cooperating with the supervisory authority of the state in which they have their registered main office or the main center of their activities in the EU;[15]
- Guaranteeing an effective and up to date security of data processing in view of new technical developments;[16]
- Notifying any personal data breach to the supervisory authority not later than 72 hours after becoming aware of it.[17]

When processing of personal data is jointly implemented by several companies, these companies are jointly liable in case of non-compliance of their obligations by one of them.[18]

Moreover, regarding subcontractors, though they are subject to the same obligations, the principal remains in charge of controlling that its subcontractor respects all of its obligations.

2.2. Specific Rules in Case of a Transfer of Personal Data Out of the EU

For the transfer of personal data to an international organization or a non-member state, in addition to those already outlined, additional obligations apply in order to guarantee the protection of European data subjects everywhere in the world.[19]

These specific rules also apply to subsequent transfers of personal data between organizations or countries outside of the EU.

Therefore, a transfer of personal data may be allowed only:

- If the European Commission affirmed, by way of a decision, that the recipient country or the recipient organization ensures an adequate level of protection;[20] or
- If in the absence of a decision of the Commission, the company has provided appropriate safeguards, and if data subjects have opposable rights and effective legal remedies.[21]

In the latter case, the appropriate safeguards may be ensured by:

- A legally binding and enforceable instrument between public authorities or bodies;[22]
- Binding corporate rules approved by a supervisor authority before the transmission of data;[23]
- Standard data protection clauses adopted by the Commission or by a supervisory authority;[24]
- A code of conduct established by a representative body of the stakeholders of a certain line of business and approved by the European Commission;[25]
- A certification mechanism established by an approved certification body.[26]

If the company issuing the personal data chooses to respect a code of conduct or to use a certification mechanism, the recipient company located in a non-member state must make a compelling and enforceable commitment "to apply the appropriate safeguards, including as regards data subjects' rights."

3. Severe Penalties in Case of Noncompliance

Penalties provided in case of non-compliance with the Regulation are of three kinds: administrative (3.1.), civil (3.2.), and criminal (3.3.) and these are cumulative.

3.1. Administrative Penalties

As it is already the case under the currently applicable rules that were replaced by the Regulation as of May 25, 2018, in case of non-compliance, the company may be subject to a financial penalty.

However, the penalty provided in the Regulation is significantly increased compared to the previous rules. The new administrative fine may reach as much as 20 million Euros or 4 percent of the relevant company's global annual turnover of the previous year,[27] whichever is highest.

Furthermore, although it is not a penalty strictly speaking, in case of a serious breach of personal data processing, the company responsible will be subject to an obligation that can be particularly harmful since it must inform all the data subjects concerned of the existence of this breach.[28]

"The purpose of the DPO is to advise the company and to monitor the processing of personal data to ensure its compliance."

This obligation to report such breach to the victims is likely to seriously affect the corporate image of the company across the EU and, consequently, to have significant repercussions on its business development.

3.2. Civil Penalties

In addition to administrative penalties, the Regulation allows civil actions against companies in case of non-compliance.

First, the Regulation opens the possibility for any data subject to introduce a civil action to obtain compensation for the prejudice suffered as a result of the non-compliance.[29]

Second, the Regulation also opens the possibility for associations dedicated to the protection of data subjects' rights to introduce a class action against non-compliant companies.[30]

3.3. Criminal Penalties

Finally, the Regulation does not prevent EU member states from prosecuting companies in case of non-compliance.

In this respect, current French criminal law remains applicable after May 25, 2018, subject to any amendment in the meantime and afterward.

It provides for penalties in case of a non-compliance with the protection of personal data which may amount, as far as individual perpetrators are concerned, to a maximum of five years imprisonment and/or a 300,000 Euros fine,[31] the latter maximum amount being multiplied by five if the perpetrator is a company.[32]

Consequently, a company that does not respect its obligation under the Regulation will possibly face a criminal fine representing 1.5 million Euros. Such penalty may be cumulated with any administrative and/or civil sanctions mentioned described in section 3.1. and 3.2. above.

4. What Should a Company Do to Ensure Compliance of Personal Data Processing Under the Regulation?

As of May 25, 2018, any company in the EU must have processing of personal data in compliance with the Regulation.

In order to ensure timely compliance, companies are recommended to conduct a legal/technical audit, in particular on all its existing contracts, to determine the number and scope of personal data processing operated by the company.

Depending on the results of the audit, it might be necessary to conduct legal and technical adjustments for all of the company's personal data processing to comply with the Regulations.

To ensure compliance of implemented solutions, the Regulation provides the development of certifications and codes of conduct to help companies better understand the proposed solutions.[33]

Throughout the company's life, it has to permanently ensure that personal data processing complies with the Regulation and actively cooperate with the supervisory authority.

Consequently, the company should seriously consider appointing a Data Protection Officer (DPO), as provided by the Regulation. The purpose of the DPO is to advise the company and to monitor the processing of personal data to ensure its compliance.[34]

The DPO, notably an individual with sound legal and technical knowledge, will be able to facilitate discussions between the company and the supervisory authority as well as the technical experts.

Endnotes

1. Article 4 of the Regulation on definitions, point 1.
2. Article 4 of the Regulation on definitions, point 2.
3. Article 5 of the Regulation regarding principles relating to the processing of personal data.
4. Article 6 of the Regulation regarding lawfulness of processing.
5. Articles 7 and 8 of the Regulation regarding the conditions for consent.
6. Article 15 of the Regulation regarding the right of access by the data subject.
7. Article 16 of the Regulation regarding the right to rectification.
8. Article 17 of the Regulation regarding the right to erasure.
9. Article 18 of the Regulation regarding the right to restriction of processing.
10. Article 20 of the Regulation regarding the right to data portability.
11. Article 21 of the Regulation regarding the right to object.
12. Article 24 of the Regulation regarding the responsibility of the controller.
13. Article 25 of the Regulation regarding data protection by design and by default.
14. Article 30 of the Regulation regarding records of processing activities.
15. Article 31 of the Regulation regarding cooperation with the supervisory authority.
16. Article 32 of the Regulation regarding security of processing.
17. Article 33 of the Regulation regarding notification of a personal data breach to the supervisory authority.
18. Article 26 of the Regulation regarding joint controllers.
19. Chapter V of the Regulation regarding transfers of personal data to non-member states or international organizations.
20. Article 45 of the Regulation regarding transfers on the basis of an adequacy decision.
21. Article 46 of the Regulation regarding transfers subject to appropriate safeguards.
22. Article 46 of the Regulation, point 2, a.
23. Article 46 of the Regulation, point 2, b.
24. Article 46 of the Regulation, point 2, c and d.
25. Article 46 of the Regulation, point 2, e.
26. Article 46 of the Regulation, point 2, f.
27. Article 83 of the Regulation regarding general conditions for imposing administrative fines.
28. Article 34 of the Regulation regarding communication of a personal data breach to the data subject.
29. Article 82 of the Regulation regarding the right to compensation and liability.
30. Article 80 of the Regulation regarding representation of data subjects.
31. Articles 226-16 to 226-24 of the French criminal code.
32. Article 121-2 of the French criminal code.
33. Articles 40 to 43 of the Regulation about codes of conduct and certification.
34. Articles 37 to 39 of the Regulation about Data Protection Officer.

François Berbinau, BFPL avocats, Paris, France