The August 6th, 2004 French Data Protection Law
Consequences for Companies

Winston MAXWELL & Julie MASSALOUX
Hogan & Hartson LLP, Paris

On August 6th, 2004 France enacted a new data protection law, sharpening the teeth of the data protection authority [1] and bringing French law into compliance with the EU Data Protection Directive [2]. Compliance is long overdue. France has for years been working under a 1978 law on data protection, originally created to address individual rights in the context of data processing by centralized mainframe computers. Many aspects of the 1978 law were ill-adapted to the world of the personal computer, let alone that of the internet. Moreover, the 1978 law did not comply fully with the EU's 1995 Data Protection Directive, which France was supposed to implement by October 25th, 1998, but did not. Because of this situation – an outdated French data protection law that did not comply with the basic EU Data Protection Directive – some French companies took a rather distant, even cynical, view of data protection compliance in France, preferring to focus instead on their compliance with the 1995 Directive itself. With the enactment of the August 6th, 2004 law (the "new law"), companies must now take French data protection rules seriously. Companies may also wish to appoint a "data protection compliance officer," a new option offered by the August 6th, 2004 law that may ease some of the paperwork linked to data protection compliance.

---

1 The *Commission Nationale de l'Informatique et des Libertés ("CNIL").*

2 Directive 95/46/EC.

Scope of the new law

The definitions of "processing" and "personal data" remain extremely broad

The new law applies to any kind of "operation" performed on personal data. The term "operation" covers practically any use of personal data – the law refers to the "collection, organization, preservation, adaptation, modification, extraction, consultation, use or communication, broadcasting, making available, interconnection, encryption, deletion or destruction" [3] of personal data.

The definition of "personal data" remains equally extensive, since it concerns information relating to a person who is identified or who may, directly or indirectly, be identified by reference to an identification number or to one or several personal elements. To determine if a person is identifiable, one should consider, "the overall means of identification to which the data controller or any other person has or may have access" [4]. Rendering data anonymous can thus be a tricky endeavour. It is often not sufficient, for instance, that names be replaced with numbers. Much more sophisticated techniques may be required to guarantee anonymity, particularly in the field of medical research involving cross-border clinical trials, for example.

The data controller need not be located in France for the law to apply

The data controller ("*responsable du traitement*") is the person or entity that defines the purposes and the methods of a particular kind of processing. If the data controller is based in France (*e.g.*, conducts business on French territory), the law automatically applies.

However, even if the data controller does not conduct business in France or in another EU country, it will be subject to the new law if it "*uses processing tools/means located in France*" [5], *i.e.*, if all or part of the processing occurs in France, through a subcontractor for example, or in some cases through the use of computers located in France. Thus, for instance, French data protection rules could apply to a foreign web merchant that sends cookies into a French person's computer, because the computer

---

[3] See, Article 2 of the 1978 law, as amended.

[4] *Id.*

[5] See, Article 5 of the 1978 law, as amended.

(the "means" of processing) is located in France. The new law nonetheless recognizes that France may be a "transit" country for the data without such a fact triggering application of the new law.

Filing obligations

One of the most burdensome aspects of the 1978 law was the obligation to file declarations for each and every kind of processing of personal data undertaken by a company: payroll, personnel management and training, security, customer relations and billing often required separate CNIL declarations. The CNIL allowed for simplified declarations in some cases, but the process was still time-consuming. The new law still imposes a filing obligation for most processing of personal data [6], but the law also empowers the CNIL to identify classes of processing that will be totally free from filing requirements, and classes of processing that will qualify for simplified filings. To ease paperwork, the CNIL will no doubt seek to exempt certain categories of routine data processing from any filing requirement, as long as the processing is of a kind that creates few risks for personal privacy and companies comply with the requirements defined by the CNIL. For the time being, no such exemption exists. However, the new law does say that certain filings may be grouped together: each time a single organization processes data for a single purpose (or several interrelated purposes), it may proceed with a single filing [7].

Data protection compliance officer

The new law exempts companies from filing obligations if the companies have appointed a data protection compliance officer [8]. The compliance officer's duty is to "ensure, in an independent manner, compliance with this law" [9]. Many details surrounding the new compliance officer remain a mystery. Will the officer be treated as a regular employee or will he be a

---

[6] Processing of sensitive data such as ethnic origin, sexual preferences and medical history requires a prior authorization by the CNIL, not just a declaration. This is addressed in the next section.

[7] See, new Article 23 II of the 1978 law, as amended.

[8] "*Correspondant à la protection des données à caractère personnel*". Note that the exemption from filing obligations is not applicable if the data in question is to be transferred outside the EU.

[9] See, new Article 22 III of the 1978 law, as amended.

"protected" employee under French labour law? The officer must possess the "necessary qualifications to perform his task," yet no one knows what the term "necessary qualifications" means. Will "necessary qualifications" mean that the CNIL must pre-approve any candidate based on his or her prior experience and training? Will the compliance officer necessarily have to live and work in France? Many multinational groups appoint a data protection compliance officer at a European level, and he or she may not live in France. Will groups be able to appoint a single data protection compliance officer for the whole group, or will each company in the group have to appoint a separate officer? If a single officer can be named for the group, will he have to be an employee (at least part-time) of each company in the group? A government decree will answer many of these questions, but until the decree is published, the CNIL has said it will not accept any notifications of the appointment of a compliance officer [10]. This makes it impossible, for the time being, to take advantage of the new procedure.

Sensitive data: CNIL authorization generally required [11]

Under the old law, the data controller had the obligation to seek CNIL approval before it could begin processing sensitive data, such as medical data, data relating to a person's racial or ethnic origin, political, philosophical or religious opinion, or sexual preferences. This remains true under the new law, which extends the list of sensitive data to, *inter alia*: genetic data, biometric data, and data relating to criminal offences, sanctions or detentions [12]. Though not expressly referred to as "sensitive data," these data are treated alike under the new law: prior CNIL approval is required before any processing. The "prior CNIL approval" procedure was also extended to three general kinds of processing that do not involve "sensitive" data *per se*, but that raise other risks for individuals:

- Processing "likely, in light of its nature, scope or purpose, to exclude persons from the benefit of a right, service or contract, in the absence of any legal or regulatory provision" [13]. This arguably seeks to protect individuals'

---

[10] *Cf.* CNIL press release dated August 9, 2004, at www.cnil.fr

[11] In general, special procedures apply where the data controller is a public entity or where the processing is performed on behalf of the French state. These procedures are not addressed in this article.

[12] See, new Article 25 I of the 1978 law, as amended.

[13] See, new Article 25 I 4° of the 1978 law, as amended.

rights to certain social benefits, such as retirement accounts or life insurance;

- Processing "designed to interconnect files held by different persons or entities, where the main purposes of such files are different" [14]; and

- Processing applied to data that includes individuals' INSEE number or requiring consultation of the national directory [15] – a situation that often comes up in connection with employee data.

The new law thus increases the number of situations where prior CNIL authorization will be required. However, where several processing acts within a company involve identical categories of data, are addressed to identical categories of data recipients, and have a single identical purpose, they may be grouped together in a single CNIL authorization. Companies may want to investigate this option upstream with the CNIL, and put in place simplified procedures from the outset.

Transferring data abroad

Like the EU Directive, the new French law prohibits sending personal data outside the EU to any country that does not assure "adequate protection". The European Commission has authority to decide whether a given non-EU country assures "adequate protection" or not, although the CNIL can in some cases challenge this finding. The law also contains the traditional exceptions to this transfer prohibition:

- *Consent.* Data can be transferred anywhere if the data subject consents. But consent is always a tricky exception to rely on, particularly when dealing with employees.

- *Necessary to perform contract.* Transfers are allowed "if necessary for the performance of a contract between the data controller and the data subject" [16] or "if necessary for the entering into or performance of a contract at the request of the data subject" [17]. These two exceptions can also be difficult to apply in practice.

---

[14] See, new Article 25 I 5° of the 1978 law, as amended.

[15] See, new Article 25 I 6° of the 1978 law, as amended.

[16] See, new Article 69 of the 1978 law, as amended.

[17] See, new Article 69 of the 1978 law, as amended.

• *Public order.* Data can be transferred if necessary for reasons of public order, life-saving or security measures. These exceptions generally do not apply to data processing by private companies.

• *Contractual clauses.* Finally, companies may transfer data outside the EU if the recipient is bound by contractual clauses or internal corporate rules guaranteeing adequate protection of the data. The CNIL is the judge of whether contractual clauses or internal corporate rules provide "adequate protection". The CNIL has already indicated under the old law that contracts conforming to the European Commission's approved contractual clauses would be sufficient for French purposes [18]. There is no reason why that position would change under the new law. But any contract that does not comply strictly with the European model would require individual review and approval by the CNIL. The new law also refers to "internal corporate rules", which could open the door to wider use of binding corporate rules instead of contractual clauses.

Labour law

Processing personal data for human resource applications requires close coordination between data protection law and French labour law. The August 6th, 2004 law on data protection changes nothing in existing French labour law. Both the labour code and the new August 6th, 2004 data protection law require that any processing of personal employee data be proportionate, *i.e.*, limited to what is necessary to achieve a legitimate objective. Labour law also imposes information and consultation obligations with the company's works council for many kinds of data processing involving employee data. In the context of biometric data, for example, a company will have to justify both to the CNIL and potentially to the company's works council and labour courts that using biometric recognition technology for employee identification is not excessive. As conditional access and identification technologies become more sophisticated, companies are tempted to implement state-of-the-art security by requiring employees to submit to fingerprint screening, or even retina scans, in order to have access to certain corporate premises or computers. Two recent CNIL opinions discuss the use of fingerprint data [19]. In the first opinion, the CNIL reviewed a request by the French public entity *Aéroports de Paris* for

[18] See, CNIL 2001 report, page 175.

[19] CNIL Deliberations n° 04-017 and 04-018.

the implementation of a biometric system to control employee access to certain high security areas in the Orly and Roissy airports. The CNIL noted that only the employees working in those areas would have to submit to such screening ; it also noted that the fingerprint was only to be included in the individual badge carried by the employee and would not be stored in a central database. In addition to other factors which the CNIL viewed as reasonable, this led the CNIL to conclude that the envisaged processing was adapted and proportionate to its purpose [20]. On the other hand, the CNIL found that the use of biometrics was not justified if the purpose of the system was exclusively to manage and control employee work hours. The Hyères hospital wanted to require six hundred employees to submit to fingerprint identification solely for purposes of controlling their work hours. The fingerprint data would be recorded in a biometric database. The CNIL's opinion with regard to that system was unfavourable because, the CNIL said, whenever one touches or handles an object, one leaves traces that may be exploited for many other unrelated purposes. Thus, the proposed processing was not proportionate to the intended objective [21].

The CNIL's new enforcement powers

One of the reasons why some companies did not pay more attention to the old law was that the CNIL lacked any credible investigative and sanctioning powers. The CNIL had to refer violations to the public prosecutor for action, meaning that only the most serious violations were sanctioned. The August 6th, 2004 law gave the CNIL new powers. The CNIL may now conduct searches ("dawn raids") between 6:00 a.m. and 9:00 p.m. on professional premises in cases where a data controller materially violates its obligations. It may also impose monetary sanctions of up to €150,000, which may be increased to EUR 300,000 in the event of a subsequent offence. The CNIL may also, among other things, order a data controller to cease and desist any processing that the CNIL deems illegal. In short, the new law considerably expands the CNIL's enforcement powers, which are in addition to court-ordered relief and criminal sanctions (a number of new offences have been added by the new law).

---

[20] See, CNIL Deliberation no.04-017 dated April 8, 2004.

[21] See, CNIL Deliberation no.04-018 dated April 8, 2004.

Transition period

What is the time frame to ensure compliance with the new law? If data processing was implemented in compliance with the old law prior to August 8th, 2004 (*i.e.*, the date on which the new law took effect), the data controller has three years, that is, until August 8th, 2007, to bring such processing into compliance with new French rules. If the characteristics of the processing are not modified, no additional formality will be required. However, with regard to (i) processing that has not been previously declared to the CNIL, (ii) processing as to which CNIL approval was requested less than two months prior to the publication of the law or (iii) processing as to which CNIL approval was requested but was still pending on the date of publication of the law, Articles 22 through 30 of the new law are applicable as of August 8th, 2004. In practice, the CNIL will inform the data controller in the event a different procedure applies to a particular kind of processing under the new law (for instance, if processing that was formerly subject to a declaration now requires prior CNIL approval).

Conclusion

Until August 6th, 2004, France lived under the ill-adapted rules of the 1978 law, which were partially non-compliant with the EU Data Protection Directive. Moreover, the CNIL lacked credible enforcement powers. The main result was that many companies simply did not comply with the old law, and focused instead on compliance with the 1995 EU Directive. The new law does relax some of the old requirements and provides practical options that should make data protection compliance easier for companies. On the other hand, violations of data protection law may now be severely sanctioned by the CNIL and by French judicial authorities. Consequently, companies will need to pay close attention to their French data protection obligations. The importance of the CNIL and of its enforcement actions is likely to increase in coming years.