France: cryptography

Exporting data from France: what does the legislation say?


The growing internationalization of data exchange brings greater challenges to those tasked with protecting both national security and individual freedoms. Olivier de Courcel and Laurent Teyssandier examine the laws governing cryptography and data export in the French Republic.

It is a fundamental tenet of democratic countries that the expression and circulation of information should be free and constitutionally protected. So it is in the French Republic. Consequently, and as a matter of principle, the export of data is also free. The only limits that can be placed upon it arise out of principles or requirements that hold equal legal value and derive from national security or public order concerns and from the protection of certain other individual liberties.

National security and public order require that the state may demand secrecy in relation to information considered to belong to the state (defence secrets) and, conversely, that it may lift secrecy on information exchanged by private individuals suspected of breaking the law (secrecy of correspondence). These national demands also require that the state controls the means for private individuals to ensure the secrecy of their own information, i.e. cryptography.

The amount of information in digital form – data – and its movement are multiplying: increasing numbers of companies are migrating to external IT providers and shared infrastructures (for example, cloud computing), public bodies are encouraged to make their data available to the public in raw form and free of charge (open data), while international data exchange, both within and between companies, is escalating. Faced with this mass of information, a second priority is emerging – that of protecting the individual and the individual's privacy in respect of data concerning the individual personally.

Given this multiplication of data and its growing internationalization in conjunction with business, increased vigilance is necessary for the protection of individuals and their privacy, while the constraints imposed by national security and public order demands are *de facto* decreased.

Data export and national security and public order interests

National security and public order impose secrecy on information considered sensitive for national defence. Thus, in France, data covered by defence secrecy may not be freely exported. Interestingly, French law does not provide any criteria defining the information concerned. However, the law does grant various ministers the power to classify information according to the level of security which should be granted to it and, consequently, the confidentiality of data concerning national defence results from an express ruling by the public authorities.

Secrecy of national defence, therefore, may cover processes, objects, documents, information, IT networks, computerized data or files of interest to national defence which have been the subject of classification measures aimed at restricting their dissemination or their access (article 413-9 of the Penal Code). Secrecy may protect intangible state property such as intellectual works, patents, raw or elaborate data. Notably, it will also apply to data belonging to French companies which work for the state, manufacturing goods on its behalf or providing services or access to, or dissemination of, materials which could harm national defence or lead to the discovery of a national defence secret.

The penalties for non-compliance with national defence secrecy are severe. Article 413-10 of the Penal Code provides for imprisonment for up to seven years and a fine of €100,000 for any custodian (either by status or profession, or by way of a function or a temporary or permanent mission) of a process, object, document, information, IT network, computerized data or file which is secret to national defence in nature, who destroys, misappropriates, abstracts, reproduces

France: cryptography

or gives access thereto to an unqualified person or brings it to the knowledge of the public or an unauthorized person.

The same penalties apply to a custodian of a defence secret party to the destruction, misappropriation, robbery, reproduction or dissemination of such items. If the custodian has acted out of imprudence or negligence, the offence is punishable by three years' imprisonment and a fine of €45,000.

Cryptography controls

To avoid being faced with data secrecy that cannot be lifted, the state also controls the means to make data secret, i.e. cryptography. Such means are used by companies to communicate both in writing (email, intranet) and verbally (audio and video-conferences, IP telephony). Commercially available solutions commonly integrate cryptography in order to protect communications, including transmissions of data from France.

Under French law, the use of cryptography is governed by articles 29 to 37 of Act no. 2004-575 of 21 June 2004 relating to the confidence in the digital economy and decree no. 2007-663 of 2 May 2007, adopted for the enforcement of some of these articles. This legislation implements Council Regulation (EC) No. 1334/2000 setting up a community regime for export controls of dual-use goods and technologies. This council regulation itself follows the 1995 Wassenaar Arrangement and the former COCOM regime. Under the act, cryptography means are defined as

> *any hardware or software designed or modified to transform data, information or signals, by means of a secret encryption key or to perform the opposite process with or without a secret key. The main purpose of cryptography means is to secure data storage and transmission, through ensuring data confidentiality, data authentication or integrity control.*

The applicable rules depend on the intended use permitted by the cryptography means. When the cryptography means exclusively guarantee data integrity and authentication (such as for an electronic signature), such means may be freely used, supplied, transferred from or to another EU Member State, or imported from or exported to any country outside the European Union (article 30 I of the Act).

When the cryptography means may be used for purposes other than to guarantee data integrity and authentication (e.g. to guarantee data confidentiality), the circulation of such means is strictly framed. Generally speaking, the use of such means is free (article 30 I of the act) though the marketing and supply of such means in France must be declared to the Prime Minister as must the transfer or importation of such means from another EU Member State or from any country outside the EU. The transfer of such means to another EU Member State and the export of such means to any country outside the EU must be authorized by the Prime Minister (article 30 III and 30 IV of the Act and article 3-1° of the decree of 2 May 2007). In each case, a few exceptions apply.

Pursuant to article 35 I 1° of the act, failing to declare to the Prime Minister the importation of means of cryptography is subject to a one-year prison sentence and a fine of €15,000 if the offender is an individual or a fine of €75,000 if the offender is a legal person. Sanctions also include prohibition of the use of cheques and payment cards, confiscation of the cryptography means that have not been declared, a ban on carrying out a professional activity in France, a five-year closure of the entity found guilty and/or a five-year ban on taking part in any public procurement contract.

Data export and individual liberties

The multiplication of data and its growing internationalization, which is inherent in the development of business, demands increased vigilance in the protection of the individual and of individuals' private lives in respect of their personal data.

Access to correspondence

The national security imperative demands that state authorities have access to private correspondence if it is regarded as suspicious. This applies to electronic correspondence as well as to postal correspondence.

By virtue of Act no. 91-646 of 10 July 1991, correspondence may be intercepted by an examining magistrate where a criminal offence or a crime punishable by imprisonment of two years or more has taken place. The administration, on the other hand, is able to intercept corresponence only at the initiative of a written, justified proposal by the minister of defence, the minister of the interior, or the minister for customs, addressed to the Prime Minister who, alone, may authorize the interception. Such interceptions at the initiative of the administration may concern only intelligence relevant to national security, the prevention of terrorism, crime and organized delinquency, the fight against combat groups and private militia, or the safeguarding of elements essential to France's scientific and economic potential.

Unlike the examining magistrate who needs neither to justify his request for interception nor to report thereupon, the administration must not only justify its decisions but also communicate them within 48 hours to the national commission for controlling security interceptions. Established as an independent administrative authority, this commission may recommend to the administration that it interrupts an interception which it considers to be illegal. The Prime Minister must report the follow-up given to his recommendations to the commission. The number of recommendations of the commission appears in a report on the conditions under which its activity is exercised which it publishes every year.

The commission controls, under the same conditions, the connection data requests that the police or gendarmerie may put to telecommunications operators. Moreover, any person having a personal and direct interest therein may ask the commission to control an interception. The administration must define and comply with an annual contingent of interceptions (less than 2,000 in 2009).

Despite this transparency, the regime governing interceptions in France does not apply to the control of transmissions using radio frequencies when it is done 'for the sole aim of defending national interests'. This notion of national interests is very broad and, as with defence secrecy, it is not based on pre-established criteria. Although this weakens the scope of the legal regime it should be noted that according to the above report, interceptions aimed at protecting France's scientific and economic potential appear to be the least numerous of all.

The benchmark legislation in this matter is Act no. 78-17 of 6 January 1978, the Data Protection Act (*Loi Informatique et Libertés*). This act was amended by Act no. 2004-801 of 6 August 2004, which transposed European directive 95/46/EC of 24 October 1995 on the protection of personal data. A European regulation is currently being adopted to reinforce the rights of natural persons concerned by the processing operations. This legislation will create new obligations for persons responsible for implementing these processing operations.

According to the provisions of article 2 of the Data Protection Act, the processing of personal data consists of any operation, irrespective of the process used, relating to information permitting the direct or indirect identification of a natural person. To this extremely broad definition, the legislation adds a list of examples of processing operations, including the

> *obtaining, recording, organization, preservation, adaptation or modification, extraction, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, deletion or destruction*

of data.

Thus, in practice, all companies are affected by this legislation since all process personal data, whether it be within the framework of their internal administration (personnel files, personnel evaluation, administration of IT resources, etc.) or of their business (client and potential client files, administration of client accounts, after-sales service, etc.).

Additionally, there are more and more companies sharing the information they hold with sub-contractors, subsidiaries or commercial partners located in other countries. Companies of a certain size no longer hesitate to entrust subsidiaries or service providers outside France with the execution of information technology-related tasks (helpdesks, for example) that were previously executed in France or in relocating their IT servers and the data they contain to countries offering a competent and cheap workforce. Others have chosen to relocate their after-sales service and hotlines. Many of these activities are farmed out to Morocco, Tunisia and other countries with a French-speaking workforce. In many cases such relocations involve the export of personal data outside France's borders.

The Data Protection Act distinguishes three hypotheses for transferring personal data abroad.

■ Personal data may circulate freely between Member States of the European Union. Since EU Member States are all subject to European directive 95/46/EC of 24 October 1995, all ensure the same level of protection of privacy and personal fundamental liberties and rights in respect of processing operations regarding personal data. Even if data transfers between Member States are not subject to particular formalities, the processing of data remains, at its base, subject to the other provisions of the Data Protection Act. For example, it must have been declared, where applicable, to the independent administrative authority responsible for ensuring compliance with the Data Protection Act (the *Commission Nationale Informatique et Libertés*, French Data Protection Authority or 'CNIL').

Iceland is added to the group of EU Member States, along with Liechtenstein and Norway, as members of the European Free Trade Association. These states are also obligated to have transposed the content of directive 95/46/EC into their national legislation.

■ The second hypothesis covers export of personal data to countries offering a so-called 'adequate' level of protection (article 68 of the Data Protection Act and article 25 of European directive 95/46/EC). The European Commission is authorized to establish the sufficient or adequate nature of protection of privacy and personal liberties and fundamental rights granted by a state. It has issued several so-called 'adequacy' rulings in favour of countries such as Argentina, Switzerland and Canada.

The European Commission has also issued an adequacy ruling in favour of the 'Safe Harbor', a particular mechanism set up by the United States, whereby U.S. companies may self-certify as adhering to a series of principles of protection of personal data and protection of privacy. This mechanism is published and administered by the United States' department of commerce.

Thus, provided the transfer of personal data is to a country where the level of data protection is acknowledged to be adequate or to a U.S. company adhering to the Safe Harbor conditions, no specific formality need be executed to export this data from France. Mention of the existence of this transfer and, where applicable, the reference to the Safe Harbor, is required in the principal processing operation prior formalities.

■ The third hypothesis concerns transfers of data to countries which are not part of the European Community and which are not considered to provide an adequate level of protection of privacy and fundamental personal liberties and rights in respect of the processing operations of personal data. Such transfers are only possible if (i) the person to whom the data relates has expressly agreed to the information being transferred or (ii) in certain exceptional cases, such as when the transfer is necessary to safeguard that person's life or is in the public interest in respect of obligations enabling the observance, exercise or defence of a right in law, the performance of a contract between the person responsible for the processing and the

France: cryptography

interested party, or if (iii) the CNIL considers that the data processing guarantees a sufficient level of protection of privacy and personal fundamental liberties and rights, notably due to contractual clauses or internal rules of which the person concerned is the subject (article 69 of the Data Protection Act).

In practice, the CNIL applies the exceptions referred to in (ii) above strictly and exceptionally. Companies are therefore strongly recommended to favour the adoption of contractual clauses or internal rules and to request the CNIL's prior authorization when they intend to transfer personal data to countries in this third category. To facilitate this approach, the European Commission has published model contractual clauses.

These questions of prior formalities before exporting data must not make one lose sight of compliance with the other provisions of the Data Protection Act. In particular, for transfers outside the European Union, companies are obliged to inform expressly those persons affected by the transfer (article 32 of the Data Protection Act). In applying decree no. 2005-1309 of 20 October 2005, companies must, therefore, communicate the following details: the countries in which the recipient of this data is domiciled; the nature of the data transferred; the purpose of the envisaged transfer; the categories of the recipients of the data; and the level of protection offered by the third countries. The company must also ensure the security of the personal data exported, which may necessitate the use of cryptography means.

Failures to comply with the Data Protection Act are liable to criminal penalties: for example, the fact of processing or having personal data processed without compliance with the legal formalities is punishable by five years' imprisonment and a fine of €300,000, including cases of simple negligence (article 226-16 of the Penal Code). The Penal Code applies the same punishment to the act of transferring or having transferred personal data to a country not belonging to the European Community if this transfer has been prohibited by the CNIL.

Other laws add regulations concerning the protection of personal data, in particular the Employment Code which, for example, requires that works councils are informed before implementing any automated processing of personnel administration, or laws specific, for example, to administrative documents, employment or consumer protection.

Conclusion

Insofar as national security and public order intervene only exceptionally in economic activities, the legal and regulatory provisions concerning data secrecy or the lifting of secrecy do not greatly interfere with the circulation of data. As a result, the provisions applicable to the processing of personal data constitute the principal restriction to exporting data by businesses located in France.

Olivier de Courcel is a partner and Laurent Teyssandier an associate at Feral-Schul/Sainte-Marie, the Paris-based technology law firm.

odecourcel@feral-avocats.com
lteyssandier@feral-avocats.com