LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Data Privacy & Security Practice

July 10, 2018 | Number 2344

France Enacts Sweeping New Data Protection Law

Pour lire cette Client Alert en français, veuillez cliquer ici.

The enactment of Law No. 2018-493 represents a significant milestone in France's implementation of the new European corpus on data protection.

Key Points:

- The new law increases fines and considerably reinforces the CNIL's powers, thereby enhancing the efficiency of the regulator's actions.
- The new law implements derogations to the GDPR that apply to French residents, regardless of the data controller's country of establishment.
- French law will further adapt to the new European corpus in the coming months.

Background

Regulation (EU) 2016/679 (the GDPR), applicable since May 25, 2018, and Directive (EU) 2016/680 (the Directive), dated April 27, 2016, have substantially enhanced the protection of personal data by imposing new obligations upon data controllers and data processors, with the aim of increasing stakeholders' accountability. For instance, data controllers must maintain a record of processing activities, execute impact assessments, implement privacy by design, improve the quality and transparency of the information provided to data subjects, and notify data subjects of data breaches if necessary, among other requirements. Data processors must maintain a record of processing activities carried out on behalf of a given data controller, enter contracts with data controllers pursuant to Article 28 of the GDPR, and assist data controllers in case of a data breach, among other obligations.

In light of this new European scheme, the French government deemed it necessary to adapt Law No. 78-17 of January 6, 1978 concerning information technology, data files, and civil liberties (the Data Protection Act), to the GDPR and the Directive's new requirements. As a result, France enacted Law No. 2018-493 regarding the protection of personal data on June 20, 2018.

Parliamentary debate

Both the National Assembly and the Senate debated the bill extensively, despite the government's initiation of the fast-track procedure on December 13, 2017. In fact, the government did not pass the bill until May 14, 2018. The bill's referral to the Conseil Constitutionnel (French constitutional court) by more than 60 senators on May 16, 2018 delayed the enactment, which was initially intended to precede the

GDPR's application on May 15, 2018. The French constitutional court rendered its decision on June 12, 2018, upholding most of the bill's original text.

Upcoming legislation

In light of the new law, the French government will need to amend Decree No. 2005-1309 of October 20, 2005, which had been enacted for the application of the Data Protection Act.

The government will also need to pass an ordinance within six months to overhaul the entire Data Protection Act, so as to enhance the act's comprehensibility and to ensure the coherence of French legislation relevant to data protection.

Main amendments to the Data Protection Act

The law's amendments to the French Data Protection Act will have broad implications for both individuals and companies. In particular, the amendments grant new powers to the French supervisory authority while clarifying France's stance on certain legal issues that the GDPR has left open to interpretation among Member States.

New powers granted to the CNIL

Advisory powers

Per its new advisory powers, the Commission nationale de l'informatique et des libertés (CNIL) will have full authority to issue soft law instruments such as guidelines, opinions, or criteria of certifications (Article 11 of the French Data Protection Act). These instruments will be based on the former single authorizations and simplified standards.

Extended investigative powers

The amendments clarify the conditions pertaining to the right to oppose a duty of professional secrecy — which, until now, the French Data Protection Act has not addressed. Under the amendments, only information covered by attorney-client privilege, by the protection of journalistic sources or by medical confidentiality, may be withheld from CNIL agents. Further, CNIL agents may now use assumed identities when carrying out online investigations.

However, the former wording of Article 44 of the Data Protection Act empowered CNIL agents to enter premises dedicated "to professional use," thereby excluding certain areas such as entrance halls or corridors. This specification has been removed in order to enhance the efficiency of on-site inspections, to the extent such inspections do not violate the privacy of private residences.

The CNIL has also gained access to a new judicial remedy under the amendments (Article 43 quinquies of the Data Protection Act), which it can use upon receiving a reclamation against a data controller or a data processor transferring personal data to a recipient in a State outside of the European Union. If the supervisory authority considers the data subject's rights and freedoms to be at risk, it can refer the case to the Conseil d'Etat (French Supreme Administrative Court) so that the latter may order the suspension of the data flows. The CNIL can also submit a question for preliminary ruling to the European Court of Justice.

Increased corrective powers

The law "regarding the protection of personal data" substantially enhances the corrective powers of the CNIL (Articles 45 and 46 of the Data Protection Act). Upon hearing of breaches of their obligations under

the applicable legislation by a data processor or a data controller, the restricted committee of the CNIL may order the following penalties:

- A warning (optional)
- An order to bring processing activities into compliance with the provisions of the Data Protection Act including, if appropriate, within a 24-hour timeframe
- A call to order
- A temporary or definitive limitation of a processing operation, a ban on said processing operation, or the withdrawal of an authorization previously granted
- An injunction to bring processing operations into compliance with the provisions of the Data Protection Act, accompanied by a fine that may not exceed €100,000 for each day the processing operations are sustained beyond the deadline
- An order to comply with the data subject's requests to exercise his or her rights pursuant to the applicable data protection legislation
- The withdrawal of a certification or the order to the relevant certification body to withdraw an issued certification
- An order to suspend data flows to a recipient in a third country or to an international organization
- A partial or full suspension of a decision approving binding corporate rules
- An administrative fine which shall, depending on the violations, oscillate between: (i) an amount of €10 million, or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher, or (ii) an amount of €20 million, or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher

The CNIL acknowledged that its controls will, at first, mainly be meant to guide the entities on their learning curve towards the implementation of the texts, if new obligations are concerned. That being said, the CNIL shall continue to rigorously investigate suspected non-compliance with the main principles regarding data protection (*e.g.,* fairness of the processing, relevance of the data processed, retention period, and data security).

Emergency procedure

The CNIL's president may refer a case to the restricted committee (Article 46 of the Data Protection Act), per an emergency procedure to be set out in a decree to be approved by the Conseil d'Etat, when:

- A violation of a provision of the GDPR or of the Data Protection Act infringes upon human identity, human rights, privacy, public, or individual liberties.
- The CNIL's president considers an intervention urgent.

The restricted committee may take one of the following measures:

- The temporary interruption of a processing operation, including a transfer of data outside of the European Union, for a maximum period of three months
- The restriction of the processing of certain personal data, for a maximum period of three months
- The temporary suspension of a certification delivered to a data controller or to its data processor
- The temporary suspension of the agreement delivered to a certification body or a body responsible for compliance with a code of conduct
- The temporary suspension of the authorization to process data concerning health when said processing operation does not meet the CNIL's criteria of certifications
- The injunction to ensure that the processing operation complies with the obligations arising out of the GDPR or the Data Protection Act or satisfies the data subject's request to exercise his or her rights, coupled with an optional periodic penalty payment that cannot exceed €100,000 per day of delay from the date chosen by the restricted committee
- A call to order
- The referral to the Prime Minister for the taking of all appropriate measures to stop the established infringements, if the processing activity concerns national security or defense or a processing activity listed by the Directive insofar as it is executed on behalf of the State

The leeway adopted under French law

The leeway's territorial scope

France chose the data subject's place of residence as the criterion to determine the territorial scope of the French leeway allowed under the GDPR. Thus, the national law applies when the data subject lives in France, regardless of the location of the data controller (except for processing operations related to the freedom of expression and information) (as per Article 5-1 of the Data Protection Act). This choice, more protective for individuals, has not been discussed or debated by parliamentarians. However, the CNIL has highlighted the practical difficulties that may arise. Indeed, the legislator could have chosen to indicate nothing in the law and, in case of litigation, let the national jurisdictions apply the classic conflict of law rules.

The age of consent of minors

After heated debates between the National Assembly and the Senate, France has determined that a minor can consent alone to the processing of his or her data in relation to information society services upon reaching the age of 15 (as per Article 7-1 of the Data Protection Act). This position, defended by the National Assembly and approved by the Conseil Constitutionnel, results from a will of coherence with other legislative acts currently applicable (for example, a 15-year-old could already require his or her doctor to not disclose medical information related to his or her situation.)

If the minor is less than 15 years old and the processing activity is based on consent, the lawfulness of the processing activity is subject to a requirement of a double consent: the consent of the minor and that of the holder of parental rights. The Conseil Constitutionnel ruled that the GDPR allows Member States to decide either that (i) the consent is given for the minor by the holder of parental rights, or (ii) the minor is authorized by the holder of parental rights to consent, which induces a double consent.

The possibility to bring a class action

The June 20, 2018 law regarding the protection of personal data broadens the possibility to bring a class action in connection with personal data (as per Article 43 ter of the Data Protection Act). If a failure of the data controller or its data processor has been established, the data subject will have the right to claim compensation alongside an association approved on a national scale that has the protection of privacy and personal data as its statutory aim, in order to compensate the material and moral damages induced by a violation of his or her personal data. The claimant may bring such a class action before the competent civil or administrative court after informing the CNIL. However, such a class action will only be possible if the event that caused the damages occurred after May 24, 2018.

Data processing related to criminal convictions, offenses, and security measures

The June 20, 2018 law regarding the protection of personal data sets out the prohibition to process criminal-related data, except for the public authority (as per Article 9 of the Data Protection Act).

The aforementioned law modifies the current legislation in order to create three other exceptions to the prohibition to process criminal and offense-related personal data, including for:

- Entities collaborating to the public service of justice (the categories of which will be defined by an implementing decree)
- Victims or defendants (either natural persons or legal entities) in order to enable them to prepare, engage in, or pursue a legal proceeding
- Users of the public information available in judicial decisions

These exceptions supplement the current exceptions made for jurisdictions, public entities, legal entities operating a public service, court officers, and legal entities monitoring copyrights. Thus, the law does not grant employers any legal basis for processing and verifying criminal records.

The exception relating to victims and defendants enshrines the Conseil Constitutionnel's reserve of interpretation, which had been first introduced in the Conseil Constitutionnel's decision No. 2004-499 of July 29, 2004 which had censored Article 9 of the Data Protection Act as modified by Law No. 2004-801, dated August 6, 2004.

The suppression of preliminary formalities

The GDPR puts an end to the main prior declarative formalities. However, the legislator chose to maintain a prior formality for the following three types of processing:

- **The processing of health data**: The new personal data law maintains a protective regime in regards to the processing of health data. The CNIL may only implement a processing activity that is compatible with the CNIL's criteria of certifications or standard regulations, and for which it has received a declaration of certified conformity. If the processing activity does not conform, it may only be implemented after being duly authorized by the CNIL (as per Article 54 of the Data Protection Act).

  The CNIL shall render its decision within two months (renewable once) after receiving the request for authorization, by a motivated decision of its president or when the case is submitted to the National Institute of Health and Informatics (INIS). However, if the CNIL does not issue an opinion within this period, the request is deemed accepted.

- **The processing implemented on behalf of the State and related to genetic data or biometric data, necessary for the authentication or the control of individuals' identity**: This processing will be subject to authorizations, by decree and after a notice of the CNIL (as per Article 27 of the Data Protection Act).

- **The processing of Social Security numbers**: The new personal data law maintains a protective regime in regards to the processing of Social Security numbers, known in France as Directory Registration Numbers (NIRs). However, the law reduces the formalities related to the implementation of a processing of the NIR (as per Article 22 of the Data Protection Act). The law suggests an upcoming framework decree, which will be enacted after a reasoned and published notice of the CNIL, to authorize the NIR's use by category of data controllers and for precise purposes.

Next steps

Under France's new personal data law, the French government will now be able to concretely implement the European corpus regarding data protection, as adopted by the European Union.

The European corpus will be completed by the adoption of the ePrivacy Regulation, to replace the ePrivacy Directive 2002/58/EC. This regulation, which the European Union Council is currently negotiating, aims at protecting the confidentiality that applies to the processing of electronic communication data related to the supply and use of electronic communication services, as well as to the information linked to the terminal connection equipment of final users. The regulation will apply to all communications, including traditional communications (which are already regulated by the former ePrivacy Directive) and new electronic communications, such as instant messaging applications. In an era of global digitalization, the regulation will affect most companies.

Latham will continue to monitor developments related to changing data protection requirements under the GDPR, both in France and around the world.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Myria Saarinen
myria.saarinen@lw.com
+33.1.40.62.20.00
Paris

Julie Ladousse
julie.ladousse@lw.com
+33.1.40.62.20.00
Paris

Elise Auvray
elise.auvray@lw.com
+33.1.40.62.20.00
Paris

Floriane Cruchet
floriane.cruchet@lw.com
+33.1.40.62.20.00
Paris

You Might Also Be Interested In

The Technology, Media & Telecommunications Review, Eighth Edition - France

GDPR Resource Center

Global Privacy & Security Compliance Law Blog