The LOPMI insurance provisions came into force on April 24, 2023

The provisions relating to the risk of cyber-attacks as set out in the French Department of the Interior's Orientation and Programming Law No. 2023-22 (known as LOPMI) enacted on January 24, 2023, came into force on April 24, 2023.

> *«Art. L. 12-10-1.-The payment of a sum under the clause in an insurance policy intended to compensate the policyholder for losses or damage caused by the breach of an automated data processing system referred to in Articles 323-1 to 323-3-1 of the French Criminal Code shall be subject to the filing of a complaint by the victim with the competent authorities no later than seventy-two hours after the victim becomes aware of the breach.*
>
> *This article applies only to legal entities and natural persons in the course of their professional activities.*
>
> *The article shall take effect three months after the enactment of this Act.»*
>
> *L'article entre en vigueur trois mois après la promulgation de la présente loi. »*

The legislator had chosen to defer (joint committee report of December 1, 20221) the entry into force of these new provisions by three months in order to give policyholders time to familiarize themselves with their obligations.

1. Who does this obligation apply to?

This obligation applies **only** to legal entities and natural persons in the course of their professional activities, and therefore not to consumers.

2. An obligation that affects all policies covering cyber-attack risks

The obligation to file a complaint applies to all coverage of cyber-attack risks including the insurance of ransomware payments.

The legislator deliberately deleted the specific reference to "the payment of ransoms" from the first bill and substituted the wording "losses and damage caused by the breach of an automated data processing system..." (National Assembly Report 436 of November 4, 2022 [2]).

[1] https://www.assemblee-nationale.fr/dyn/16/rapports/343/l16b0590_rapport-fond#

[2] https://www.assemblee-nationale.fr/dyn/16/rapports/cion_lois/l16b0436_rapport-fond#

A reading of the report of the National Assembly's law commission no.436-4 from November 2022 confirms there is nothing in positive law (European law, legislation of OECD countries, French Civil Code, French Insurance Code, French Criminal Code and French case law) to preclude the insurability of ransom payments. This position was confirmed by the Legal High Committee for Financial Markets of Paris[3] (report of January 28, 2022). Only the case of a ransom payment made with the knowledge that the funds provided would be used to commit a terrorist act (article 421-2-2 of the French Criminal Code[4]) can preclude the insurability of this risk.

The reference to Articles 323-1 to 323-3-1 of the French Criminal Code excludes from this obligation the consequences of computer security incidents having an accidental cause or resulting from an error. **They do therefore refer to the consequences of a cyber-attack.**

3. Confirmation of the insurability of ransom payments sets guidelines for the compensation of victims of cyber-attacks

The Law Commission of the National Assembly (report 436 - page 48) confirms that this is about confirming the insurability of ransoms and not its legalization. In fact, ransom payments have always been insurable provided the victim and their insurer complied with the legislation on breaches of the terrorism financing laws provided for in Article 421-2-2 of the French Criminal Code.

4. A 72-hour deadline to comply with this new obligation

The choice of the length of this period results from a balance between the interests of the victim (who must be given time to respond) and the needs of the investigation.

This choice, initially set at 24 hours, was extended to 48 and then 72 hours.

This new system makes the payment of insurance compensation conditional on "the filing of a complaint by the victim with the competent authorities no later than seventy-two hours after the victim becomes aware of the breach." It enables information to be provided more easily to the security forces and the judicial authority and facilitates the investigations. It would therefore contribute to a better response to a cyber-attack through the cross-referencing of complaints and clues, as a cyber-attack rarely strikes just one victim. It would also allow for a better understanding of the techniques and methods used by cybercriminals (Senate Report no.19 page 32 - October 5, 2022 / National Assembly Report no.436 page 48 - November 4, 2022).

The starting point:

As for the starting point of this time limit for filing a complaint, the legislator has opted for **the time of «the discovery of the offense by the victim»** instead of "the time of payment of the ransom" or "the time of the attack". This is to take into account the difficulties for victims in determining the exact moment of the start of a cyber-attack. This wording aims to bring legal certainty to the judicial system. It draws on the provision of the NIS 2 Directive which provides for incident notification within 72 hours of "the discovery of the security incident".

Depending on the size and number of the policyholder's workforce, the time limit for filing a complaint will begin to run when the legal representatives or their delegates (risk manager, CISO, Company Secretary, etc.) are informed or become aware that their company has been the victim of a criminal offence (cyber-attack).

[3] https://www.banque-france.fr/sites/default/files/rapport_45_f.pdf

[4] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006418433

5. What insurance policies does this apply to?

The restriction to the payment of ransoms was deliberately removed by the Law Commission of the National Assembly (National Assembly Report 436 page 51[5]) to extend this obligation to all insurance reimbursements.

This article applies to policyholders who benefit from cyber risk coverage (financial losses or cyber crisis management) as part of their cyber risk insurance or which may be appended to other insurance policies (e.g. cyber crisis management component in a PI policy).

6. How to file a complaint

In the event of a cyber-attack, we recommend including your complaint in your crisis management plan, taking care to:

- Preserve all visible traces of the attack (photos, screenshots, etc.),
- List all actions taken as a result of the attack in chronological order,
- Provide or keep available as much evidence as possible (files, photos, pictures, videos, USB sticks, CDs/DVDs, hard drives, etc.).

The victim must file a complaint at a gendarmerie or police station within 72 hours of learning of the incident.

Information on how to file a complaint is available at the link below:
https://www.masecurite.interieur.gouv.fr/fr.

If the company, registered in France and insured under a French insurance policy, is the victim of a cyber-attack abroad, we recommend filing a complaint both:

- In France within 72 hours,
- In the country of operations within 72 hours.

By doing so, the obligation to file a complaint will be met.

[5] https://www.assemblee-nationale.fr/dyn/16/rapports/cion_lois/l16b0436_rapport-fond#

DiotSiaci

SIACI SAINT HONORE – DIOT-SIACI Group – Insurance and reinsurance broker

Registered office: Season - 39, rue Mstislav Rostropovitch - 75815 PARIS CEDEX 17 - FRANCE – Tel: +33 (0)1 4420 9999 - Fax: +33 (0)1 4420 9500.

A French Société par actions simplifiée (SAS) – Capital: €120,555,961.60 – Registered with the Paris Trade and Companies Register under number 572 059 939 – APE 6622 Z – VAT No.: FR 54 572 059 939.

ORIAS No.: 07 000 771 (www.orias.fr) – Regulated by the ACPR - 4 place de Budapest - CS 92459 - 75436 PARIS CEDEX 09 - FRANCE.

Complaints: SIACI SAINT HONORE - Service réclamations - 23, allées de l'Europe - 92587 CLICHY CEDEX - FRANCE.

DIOT – DIOT-SIACI Group – Insurance and reinsurance broker

Registered office: Season - 39, rue Mstislav Rostropovitch - 75815 PARIS CEDEX 17 - FRANCE – Tel: +33 (0)1 44 79 62 00.

A French Société par actions simplifiée (SAS) – Capital: €1,831,008 – Registered with the Paris Trade and Companies Register under number 582 013 736 – VAT No.: FR 92 582 013 736.

ORIAS No.: 07 009 129 (www.orias.fr) – Regulated by the ACPR - 4 place de Budapest - CS 92459 - 75436 PARIS CEDEX 09 - FRANCE.

Complaints: reclamations@diot.com – www.mediation-assurance.org