MOLITOR
Avocats à la Cour

One incident, many clocks.

Coordinating breach notifications under GDPR, NIS2, DORA and beyond.

The Friday 11:40 pm incident.

Julien Pétré
Counsel, MOLITOR Avocats à la Cour (Luxembourg)

INPLP · Amsterdam · 21 November 2026



The cast and the incident

THE CAST

PayLux S.A.

- Luxembourg e-money institution

US-listed parent

- Non-EU group parent

Non-EU cloud provider

- Hosts PayLux's payment app

Non-EU software vendor

- Supplies the (vulnerable and on-premise) software

THE INCIDENT

Ransomware enters through the cloud service, exploiting the vendor's software flaw.

- **Customer data is taken.**
- **The payment app goes down.**

Friday 20 November, 11:40pm CET, PayLux becomes aware of the incident.

Saturday 21 November, 01:40am CET, PayLux classifies the incident as major (from a DORA perspective).

Two regimes and four audiences

Audience	DORA	GDPR
Authorities and timing	Financial supervisory authority (CSSF) ➢ Initial: within 4h of classification as major incident, and no later than 24h after awareness ➢ Intermediate: 72h after initial filing ➢ Final: 1 month after latest intermediate	Data protection supervisory authority (CNPD) ➢ Unless unlikely to result in a risk, without undue delay and, where feasible, within 72h after awareness + phased information where necessary
Clients / data subjects	Clients ➢ Without undue delay if a major incident affects their financial interests	Data subjects ➢ Without undue delay if the breach is likely to result in a high risk

Triggering events

- **DORA:** major-incident classification.
- **GDPR:** awareness of a personal data breach.

The same weekend, with and without DORA relief

- Awareness: Friday 11:40pm CET.
- Major classification: Saturday 01:40am CET.

PayLux filing	No DORA weekend relief	Eligible DORA weekend relief
DORA initial	Saturday 21 November, 05:40am	Monday 23 November, 12:00pm
DORA intermediate	Tuesday 24 November, 05:40am	Thursday 26 November, 12:00pm
GDPR (CNPD)	Monday 23 November, 11:40pm	Monday 23 November, 11:40pm

No relief for credit institutions, CCPs, trading venues, other NIS2 essential/important financial entities, or entities subject to a notified CSSF exclusion.

MOLITOR
Avocats à la Cour

Non-EU suppliers: what they must report

Supplier	Route and timing	Content of the filing	Information to PayLux
Cloud provider (NIS2)	**To whom?** ➢ Authority/CSIRT of the EU Member State of its EU representative. **When?** ➢ 24h / 72 h / 1 month (+interim report on request)	**Early warning (24h)** ➢ Suspected malicious acts and possible cross-border impact **Notification (72h)** ➢ Severity, impact and indicators of compromise **Final report (1 month)** ➢ Root cause, mitigation measures and cross-border impact	**By law** ➢ Notice to service recipients "*where appropriate*", without undue delay, and no right to copy of the filing **By contract (DORA Art.30)** ➢ Incident assistance and notice of material developments
Software vendor (CRA)	**To whom?** Coordinating CSIRT + ENISA (via ENISA platform) **When?** 24h / 72h / 14 days after a fix (1 month in the incident track)	**Warning (24h)** ➢ The Member States where the product is available **Notification (72h)** ➢ Product, vulnerability, exploit and available mitigations **Final report (14 days/1 month)** ➢ Severity, impact, known attacker and corrective measures	**By law** ➢ Impacted users (all users where appropriate) + mitigations, and CSIRT may step in **By contract (DORA Art.30)** ➢ As for the cloud provider, if support/updates are contracted

MOLITOR
Avocats à la Cour

The consequences of a missed or insufficient notification

Actor / regime	Maximum fine	Key elements
PayLux / DORA	€5m or 10% of total annual turnover	➢ Covers DORA Arts 17–19 and 23 (incident handling and reporting) ➢ Individuals (incl. management): up to €5m ➢ Public statement ➢ Obstructing the CSSF: €250–250,000
PayLux / GDPR	€10m or 2% worldwide annual turnover, whichever is higher	➢ Covers notification to CNPD (Art. 33) and data subjects (Art. 34) ➢ Compensation claims also possible
Cloud / NIS2	➢ Essential: €10m or 2%, whichever is higher ➢ Important: €7m or 1.4%	➢ Fined where its EU representative sits (ILR if in Luxembourg) ➢ No NIS2 fine if GDPR fine for the same conduct ➢ Essential entity: temporary CEO ban possible
Vendor / CRA	€15m or 2.5% worldwide turnover, whichever is higher	Reporting applies since 11/09/2026, but fines applicable only from 11/12/2027

MOLITOR
Avocats à la Cour

PayLux's playbook: seven decisions before, during and after

01	**BEFORE · Contracts 4h-ready?**	Supplier incident notice in hours, assistance and CSSF cooperation (DORA Art. 30) + knowledge of where the cloud's EU representative sits.
02	**BEFORE · Who decides at 2am?**	Named classification team with deputies, contact list for CSSF/CNPD, pre-drafted templates + rehearsal of a weekend incident with the board.
03	**DURING · When did we know?**	Log awareness (Fri 11:40pm) and major classification (Sat 01:40am) + classify promptly and record the reasoning.
04	**DURING · Which clocks are running?**	CSSF 4h/24h (check weekend relief), CNPD 72h, clients and data subjects without undue delay + if late, tell the CSSF/CNPD before the deadline.
05	**DURING · Who receives what?**	One fact sheet for four audiences + document any decision not to notify.
06	**DURING · Do supplier facts match ours?**	Request supplier facts, reconcile with their notices to users or authorities (if any), preserve evidence, explain corrections in updates.
07	**AFTER · What do we close and fix?**	Final reports + root-cause review, remediation, board report, contract and playbook updates.

What's next: one portal, same clocks?

Commission proposal of 19 November 2025 - DIGITAL OMNIBUS

Digital Omnibus	Impact on PayLux's Friday-night incident
One ENISA single-entry point for, among others, NIS2, GDPR and DORA ("report once, share many")	One interface for the CSSF (DORA) and CNPD (GDPR) filings
DORA Art. 19: major ICT incidents reported to the competent authority via the single-entry point	Single entry-point but still the same clocks
GDPR Art. 33: notify only if likely high risk, within 96h (reasons if later), via the single-entry point	Notification only if high risk likely. The CNPD still notified but by Tue 24 Nov 11:40pm instead of Mon 11:40pm
NIS2 reports via the single-entry point: a CRA severe-incident report counts as NIS2 reporting	A severe-incident report under the CRA counts as NIS2 reporting, provided it contains the information NIS2 requires (“once-only” principle). No practical impact: the cloud provider (NIS2) and the vendor (CRA) are different entities, so each keeps its own report.

MOLITOR
Avocats à la Cour

Three takeaways

01 Map each clock from its own trigger.

DORA runs from classification (4h, max. 24h after awareness), the GDPR from awareness (72h). Weekend relief can move the CSSF deadline, never the CNPD's deadline.

02 Suppliers' reports are not PayLux's report.

The cloud provider (NIS2) and vendor (CRA) report to their own authorities and PayLux sees none of it: DORA Art. 30 contract terms are its route to the facts.

03 Prepare before Friday night: missed clocks cost.

Named decision-makers, templates and a rehearsed weekend scenario. DORA fines reach 10% of (group) turnover. The Digital Omnibus brings one portal, not one clock.

MOLITOR
Avocats à la Cour

Discussion: three open questions

01 Should weekend relief exist? Should the GDPR and NIS2 have it too?

DORA moves a weekend deadline to Monday 12:00pm while the CNPD clock keeps running: is that justified for a privacy regulator?

02 One incident, one narrative?

The DORA authority gets facts on Saturday, the GDPR's authority on Monday. How do you keep both filings consistent, and should the first report shape the second?

03 Who controls the story: PayLux or its suppliers?

Suppliers may notify users and authorities first. Can contracts give PayLux a right to review supplier notices, and is that realistic with hyperscalers?

MOLITOR

Avocats à la Cour

More about us

Your dedicated contact



Phone

(+352) 297 298 75

Email

julien.petre@molitorlegal.lu

Adresse
8, rue Sainte-Zithe
P.O. Box 690
L-2016 Luxembourg

Phone
(+352) 297 298 1

Mail & web
contact@molitorlegal.lu
www.molitorlegal.lu