FROM THE IUSTORIA BLOG

Cyberattack or Data Breach at Your Company: What to Do in the First 72 Hours

> *Encrypted servers, a ransom note, a leaked customer database. What to report to the ÚOOÚ within 72 hours, when NÚKIB needs a report within 24, what to tell insurers and partners, and why not to pay.*

IUSTORIA TEAM

5 November 2026 · 12 min read

On Monday morning, the files on the shared drive will not open and the screens show a message saying the data has been encrypted and where to send the ransom. Or a customer calls to say that someone is offering their details from your database for sale online. The first call goes to your IT administrator, and rightly so. What we see at our firm, though, is that nobody thinks of the legal side until a week later, once the servers are running again. By then the notification deadlines have passed, and the traces that could have helped the company defend itself before the authority, the insurer or a court have vanished with the reinstallation.

The first three days are not only about technology. They also decide what to report and to whom, who needs to be informed, how to secure the evidence and whether to pay. We go through the time limits under the General Data Protection Regulation (GDPR) and under the new Czech Cybersecurity Act, what to expect from your insurer and business partners, and who is responsible for the decision on a ransom.

The first hours: stop the attack and keep the traces

The National Cyber and Information Security Agency (NÚKIB) recommends that, once ransomware is detected, devices be disconnected from the network and switched off only if there is no other way, because switching them off destroys traces held in memory. The backup server is disconnected first, so that the attack does not reach the backups too. NÚKIB further recommends taking bit-for-bit images of the affected systems, collecting the operating logs and samples of the malicious code, and communicating outside the compromised network, by phone for example. The attacker may still be reading the company's email.

From a legal point of view, we add two things. First, keep an incident log from the very first minute: when the attack was detected and by whom, what happened, who decided what and why. The moment of detection starts the time limits running, and a controller of personal data must document every personal data breach, even one it ultimately does not notify (Article 33(5) GDPR). Second, do not reinstall anything until you have the copies. The police, the insurer and the Office for Personal Data Protection (ÚOOÚ) all need the traces of the attack. Above all, though, you will need them yourself when you have to prove that the company's security was adequate.

Personal data breach: notify the ÚOOÚ within 72 hours

A personal data breach covers not only a leak of personal data but also its accidental or unlawful destruction, loss or alteration (Article 4(12) GDPR). Ransomware that encrypts a customer database or payroll records is therefore a personal data breach even if the attacker took nothing away. Both the ÚOOÚ and the European Data Protection Board (EDPB) classify this as an availability breach.

Not every such breach has to be notified, however. The EDPB gives the example of a small company that kept its data encrypted, restored it from a working backup within a few hours without any interruption to its business, and whose log analysis showed with certainty that the attacker had copied nothing; the risk to people was un-

likely there, and documenting the incident was enough. For a company that spent five working days restoring its data from paper records, the EDPB considers notification necessary. And where the controller is unsure how far the attacker got, the EDPB says it should assume the worse scenario.

The controller notifies the breach to the ÚOOÚ without undue delay and, where feasible, not later than 72 hours after having become aware of it. The only exception is a breach that is unlikely to result in a risk to people's rights and freedoms. If it notifies later, it must give the reasons for the delay (Article 33(1)). According to the EDPB, the controller has "become aware" of the breach as soon as it has a reasonable degree of certainty that an incident has occurred and personal data has been compromised. The time limit is counted in hours and does not pause for the weekend.

Do not wait for IT to finish its analysis. If you do not yet know the full extent, notify what you know and provide the rest in phases; the Regulation expressly allows this (Article 33(4) GDPR). An incomplete notification filed on time is better than a complete one with an apology for the delay.
The notification must describe the breach, including the categories and approximate number of people and records concerned, give the contact details of the data protection officer or another contact point, and describe the likely consequences and the measures taken (Article 33(3)). The ÚOOÚ provides an electronic form for this. The completed form can be sent via a data box (*datová schránka*, the Czech state electronic mailbox for official communication; the ÚOOÚ's ID is qkbaa2n), by post or by email to posta@uoou.gov.cz. An email, however, must bear a recognised electronic signature (*uznávaný elektronický podpis*); otherwise the authority treats it as a proper notification only if you confirm it with a hand-signed form sent by post or delivered in person. The data box is the safest route.

Responsibility lies with the controller, meaning whoever decides on the processing. If the attack happened at a supplier, such as a cloud provider or a payroll software provider, that supplier, as processor, must notify you without undue delay (Article 33(2)) and assist you in meeting your obligations (Article 28(3)(f)). The notification to the ÚOOÚ, however, is yours to make. Breaching these obligations can lead to a fine of up to EUR 10 million or 2% of total worldwide annual turnover, whichever is higher (Article 83(4)).

In November 2025, in what is known as the digital omnibus, the European Commission proposed extending the time limit to 96 hours and requiring notification only of high-risk cases. As at 6 November 2026, the proposal had not been adopted, and the 72 hours still apply.

When to write to the people whose data leaked

If the breach is likely to result in a high risk to people's rights and freedoms, the controller must also inform them directly, without undue delay (Article 34(1) GDPR). Typically this means leaked passwords, personal identification numbers, bank account numbers, health data or anything else that can be misused for fraud. The communication must be written in clear and plain language and include a contact point, the likely consequences and the measures taken (Article 34(2)). We recommend also telling people what to do: change their passwords, distrust emails and phone calls that invoke your company, and keep an eye on their account activity. Fraudsters like to use leaked data to make their messages look convincing.

You need not inform people if the data was encrypted and unintelligible to the attacker, if you have taken measures that make the high risk no longer likely to materialise, or if informing them would involve disproportionate effort. In the last case, however, you must issue a public communication instead (Article 34(3)). The ÚOOÚ can order you to inform them (Article 34(4)).

Anyone who has suffered material or non-material damage as a result of an infringement of the Regulation has the right to compensation (Article 82(1)). In its judgment of 14 December 2023, Natsionalna agentsia za prihodite, Case C-340/21, the Court of Justice of the EU examined an attack on the Bulgarian tax administration after which the data of more than six million people appeared online. It held that a leak caused by an attack by third parties does not in itself mean that the controller's measures were inappropriate. In a dispute over compensation, however, the controller bears the burden of proving that they were appropriate, and it is not exempt from liability merely because the leak was caused by the attacker. The fear of possible misuse of one's data can in itself be non-material damage, provided it is well founded in the circumstances (operative part, points 1, 3, 5 and 6; paragraph 85). For a company, this means its defence rests mainly on documentation: security policies, records of training, updates and backups, and the incident log.

The new Cybersecurity Act: does it apply to you?

Act No. 264/2025 Coll., on Cybersecurity, which transposes the EU's NIS 2 Directive into Czech law, has been in force since 1 November 2025. It applies to providers of regulated services in 15 sectors, ranging from energy, manufacturing and food through transport, water, waste management and healthcare to digital services (Section 4(1)). As a rule, it covers medium-sized and large enterprises; a small enterprise only if it is of particular importance to the state, and some services are registered by the agency regardless of size (Section 5). The specific services are set out in Decree No. 408/2025 Coll., on Regulated Services. Do not wait for the agency to contact you: the provider must notify its service to NÚKIB itself, no later than 60 days after the day on which it met the conditions (Section 6(1)). The size of the enterprise is assessed together with the companies in its group, so the Act may also apply to a small subsidiary of a large group; the only group companies left out of the count are those whose technical assets are entirely separate from the ones the company uses to provide the regulated service (Section 7(c)). A company that has recently grown, taken on a new activity or joined a group should check this straight away.

A provider in the higher-obligations regime (*režim vyšších povinností*) reports incidents to NÚKIB, and a provider in the lower-obligations regime (*režim nižších povinností*) to the National CERT, and only those with a significant impact on the service (Section 15(1) to (3)). The time limits are shorter than under the GDPR: an initial report no later than 24 hours after the incident is detected (Section 16(1)). This is followed within 72 hours by a notification with an initial assessment, and within 30 days of that by a final report. In the lower-obligations regime this applies to every reported incident with a significant impact on the service; in the higher-obligations regime it applies where NÚKIB states that the incident has a significant impact on the state's cyberspace (Section 16(2) and (3)). Reports are filed through the NÚKIB Portal (Section 16(4)). The provider must start reporting

no later than one year after the registration decision is delivered to it (Section 15(4)). Failing to do so can lead to a fine of up to CZK 250 million or 2% of worldwide turnover in the higher-obligations regime, and up to CZK 175 million or 1.4% in the lower-obligations regime, whichever is higher (Section 59(4)).

Reporting to NÚKIB and notifying the ÚOOÚ are two separate obligations, and one does not replace the other. The authorities merely exchange information so as not to penalise a breach of the same obligation twice (Section 64(5)). And a company to which the Act does not apply may report an incident to NÚKIB voluntarily (Section 15(5)); the Act provides that the agency or the National CERT will respond to such a report too and offer methodological help (Section 17(5)).

The police, the insurer and business partners

An attack is usually the criminal offence of unauthorised access to a computer system and interference with it (Section 230 of the Czech Criminal Code), and the ransom demand is extortion on top of that (Section 175). NÚKIB, too, recommends contacting the police. A criminal complaint also shows that the company was the victim, and both the insurer and your partners will ask about it.

If the loss is covered by insurance, notify the insurer of the insured event without undue delay, give a truthful explanation, submit the documents and follow the procedure agreed in the policy (Section 2796(1) of the Czech Civil Code). The last part is easy to overlook. Before you hire a forensics firm or start dealing with the attacker in any way, read your policy conditions; whatever they say about the procedure after an insured event binds you as well. How long the insurer may investigate a claim and when you can ask for an advance payment is explained in our guide on claims investigation and advances (in Czech).

Your business partners matter from two angles. If the attack prevents you from delivering on time, you are liable for the damage, and only an extraordinary, unforeseeable and insurmountable obstacle will release you (Section 2913(2) of the Civil Code). We would not bet today on a court treating a cyberattack as such an obstacle: attacks are common, and companies are expected to defend against them. Go through your contracts, then, to see what they say about force majeure, incident notification and deadlines. What a good force majeure clause should look like is covered in our article Five Contract Clauses That Can Save You Millions (and That Nobody Reads). Data processing agreements often set their own notification deadlines, as do the contracts that a provider of a regulated service concludes with its suppliers; for the latter, the Cybersecurity Act expressly requires security requirements to be included (Section 13(5)). Write to partners whose data or systems may have been affected promptly and factually, saying what happened and what they should do. Guesses about who is to blame and reflections on what could have been done better have no place in such a letter.

The ransom: a decision for which management is answerable

NÚKIB recommends not paying a ransom under any circumstances. Payment encourages attackers to strike again, nothing guarantees that they will unlock or delete the data, unlocking it does not remove the malicious code, and from a legal point of view paying may breach the duty of care of a prudent manager (*péče řádného*

hospodáře). The last reason concerns the managing director or board member personally. They must perform their office with the necessary loyalty as well as the necessary knowledge and care (Section 159(1) of the Civil Code), and in a dispute it is up to them to prove that they did so (Section 52(2) of the Czech Business Corporations Act). They are protected by the business judgment rule: a director who could, in good faith, reasonably assume that they were acting on an informed basis and in the defensible interest of the company passes the test (Section 51(1)).

If management is considering paying, perhaps because the company will not survive without its data, the decision needs a basis: an assessment of whether and how quickly operations can be restored from backups, a quantification of the losses, the insurer's position, and a record of why management decided as it did. More on a managing director's liability can be found in our guide to what a managing director is liable for (in Czech).

Two things always apply. The money must not go to persons and groups on the EU sanctions list; the Union has its own sanctions regime for cyberattacks (Article 3(2) of Council Regulation (EU) 2019/796), and breaching international sanctions on a larger scale is a criminal offence (Section 410 of the Criminal Code). The attacker, of course, does not introduce themselves. Before management pays, a forensics firm should first identify which group is behind the attack, the findings should be checked against the sanctions lists, and the result belongs in the record of the decision. And paying changes nothing about the notification obligations: the breach has already happened, and nobody can verify the attacker's promise that the data has been deleted.

Write down today, on a single page, who makes the decisions during an attack, the phone numbers of management, the IT administrator, the insurer and your lawyer, and how to notify the ÚOOÚ. Keep it outside the company's systems, on paper for example.
Check whether your service is listed in Decree No. 408/2025 Coll. If you meet the conditions of the Cybersecurity Act, you must notify NÚKIB yourself within 60 days.
In your contracts with IT and cloud suppliers, check within how many hours they must report an incident to you and what information they will send you. Without it, you cannot put together a notification to the ÚOOÚ.

At a glance

Question	Answer	Provision
Is encryption of data by ransomware a personal data breach?	Yes, it is a loss of availability; it must be notified unless the risk to people is unlikely	Article 4(12), Article 33(1) GDPR
Deadline for notifying the ÚOOÚ	Without undue delay, where feasible within 72 hours of becoming aware; later only with reasons	Article 33(1) GDPR
When to inform the people affected	Where a high risk is likely, without undue delay	Article 34 GDPR
Fine for breaching notification obligations	Up to EUR 10 million or 2% of worldwide turnover	Article 83(4) GDPR
Reporting under the Cybersecurity Act	Initial report within 24 hours; for an incident with a significant impact, a notification within 72 hours and a final report within 30 days of the notification	Section 16 of Act No. 264/2025 Coll.
Notifying a regulated service to NÚKIB	Within 60 days of meeting the conditions	Section 6(1) of Act No. 264/2025 Coll.
Notifying the insurer	Without undue delay and following the procedure in the policy	Section 2796(1) of the Civil Code
Ransom	NÚKIB advises against paying; payment to persons on the sanctions list is prohibited	Article 3(2) of Regulation (EU) 2019/796

Dealing with an attack or a data breach right now? We will help you decide what to report and to whom, prepare the notification to the ÚOOÚ, the communication to the people affected and the letters to your insurer and partners, and give management a sound basis for decisions that will be scrutinised later. We handle data protection and cybersecurity as part of our IT compliance practice. Get in touch.

Conclusion

The legal time limits after a cyberattack run regardless of when the systems are back up: 72 hours for the ÚOOÚ, 24 hours for NÚKIB or the National CERT for regulated services, and without undue delay for the insurer. A company that secures the traces in the first hours, keeps a log and notifies on time, even with incomplete information, will have something to defend itself with before the authority, the insurer and the court.

A company that knows in advance whether it falls under the Cybersecurity Act and what its suppliers promise it in their contracts will not have to work that out in the middle of an attack.

Sources

- Regulation (EU) 2016/679 of the European Parliament and of the Council, the General Data Protection Regulation, Article 4(12), Article 28(3)(f), Article 33, Article 34, Article 82 and Article 83(4).
- Act No. 264/2025 Coll., on Cybersecurity, Sections 4 to 8, 13, 15, 16, 17, 59 and 64 (as in force from 1 November 2025).
- Decree No. 408/2025 Coll., on Regulated Services.
- Act No. 89/2012 Coll., the Civil Code, Sections 159, 2796 and 2913.
- Act No. 90/2012 Coll., on Business Corporations, Sections 51 and 52.
- Act No. 40/2009 Coll., the Criminal Code, Sections 175, 230 and 410.
- Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, Article 3.
- Judgment of the Court of Justice of the EU of 14 December 2023, Natsionalna agentsia za prihodite, Case C-340/21.
- European Data Protection Board, Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, and Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, Version 2.0, Cases No. 01 and 02.
- NÚKIB, Ransomware: recommendations for mitigation, prevention and response, version 1.2 of 22 May 2023, section 4.
- Office for Personal Data Protection, Personal data breach (uoou.gov.cz).

This article is for information only and does not constitute legal advice. It reflects the law as at the date of publication; whether a particular incident must be reported, and to whom, depends on which data and services it affected and on whether the company falls under the Cybersecurity Act.

Cyberattack or Data Breach at Your Company: What to Do in the First 72 Hours

IUSTORIA team · Published 5 November 2026

https://www.iustoria.cz/en/blog/cyberattack-or-data-breach-first-72-hours/

This text is protected by copyright. Sharing the document whole and unaltered is welcome; reuse of parts in other texts requires attribution. © IUSTORIA, advokátní kancelář, s.r.o.