I HAVE AN INCIDENT · PRELIMINARY ASSESSMENT · SHORT PLAN

Incident action plan

Encrypted files, ransom demand · detected Sat 14 Nov 2026, 08:33 Polish time · essential entity under the Polish KSC Act · data controller

Preliminary assessment based on the user's answers · law as at 11 Nov 2026. The pages with the short plan are enough to act on; the documentation for the file follows. All times are Polish time (CET/CEST).

NEAREST DEADLINE

By Sun 15 Nov 2026, 08:33 Polish time

Applies to: KSC · Submit an early warning. At the time the plan was downloaded: 17 h 59 min left. Obligations (preliminary): 7; of these, with a deadline counted in hours: 3. To be established and recommendations: 2. Information: 0.

Deadlines and result items

By when	Action
Sun 15 Nov, 08:33 17 h 59 min left	KSC **Submit an early warning**
Tue 17 Nov, 08:33 2 d 17 h left	KSC **Notify the significant incident (incident notification within 72 h)**
Tue 17 Nov, 10:33 2 d 19 h left	GDPR **Notify the breach to the President of UODO (the Polish data protection authority)**
without undue delay — do not wait for 72 h to pass	GDPR **Communicate the breach to the data subjects — preliminarily, the risk is high** Assessment based on the type of data; exception: the measures taken after the event have made the high risk no longer likely (Article 34(3)(b) GDPR) — decided by the controller
on an ongoing basis	GDPR **Record the breach in the breach register**
one month from the day of the incident notification	KSC **Submit a final report**
without delay — the Act sets no deadline	KSC **Inform the users of your services**

Counted from the time given in the questionnaire. When detection and becoming aware took place is assessed by the controller or by the entity covered by the KSC Act. The deadline is the last possible moment. Notify earlier whenever you can. Full descriptions of the items with their legal bases are in the “Documentation for the file” part.

To be established and recommendations (no deadline counted in hours)

- KSC · Competent CSIRT: CSIRT NASK — check before notifying
- Law enforcement · Consider reporting to the police or the public prosecutor

First aid

- [x] Write down when the event was detected and who noticed it. From now on, keep a short log: who did what and when.
- [x] Disconnect infected computers from the network (cable and Wi-Fi). Do not switch them off.
- [ ] Disconnect backup drives from the network before they are encrypted too.
- [ ] Do not pay the ransom and do not contact the criminals.
- [ ] Change administrator passwords from a clean device.
- [ ] Check whether data was stolen before the encryption (a message from the criminals, unusual outbound traffic). This changes the assessment of the breach.
- [ ] Do not delete anything. Keep the evidence: screenshots, emails with headers and logs.
- [ ] Inform management. The decision to notify is the organisation's, and deadlines run at weekends too.
- [ ] If you have cyber insurance, report the event to the insurer. Policies often require prompt notice.

NEED HELP?

Call LabLogic: +48 504 920 875

Phone answered on working days, 8–16 Polish time. If a deadline expires within a few hours, do not wait for my call. Notify on your own and complete the notification later.

I HAVE AN INCIDENT · DOCUMENTATION FOR THE FILE

Full result and reasons

Each result item with its legal basis, the reasons, the content of the notifications, the incident card, fields to complete and the wording of the provisions. Attach this part to the incident documentation.

Result step by step

OBLIGATIONS

KSC **Submit an early warning**

You notify through S46, the ICT system under Article 46 of the KSC Act run by the minister responsible for computerisation. An early warning does not require knowing the cause. You give the entity's details and contact persons, the moment the incident occurred and was detected, and whether it may have been caused by unlawful action and whether it affects other EU Member States. You may ask for guidance and technical support. Addressee: CSIRT NASK — details in the item "Competent CSIRT: CSIRT NASK".

by Sun 15 Nov 2026, 08:33 Polish time

Legal basis: Article 11(1)(4) of the KSC Act, Article 11(2) of the KSC Act, Article 12(1) of the KSC Act, Article 12(2) of the KSC Act, Article 44(1) of the Act of 23 January 2026 (Journal of Laws 2026, item 252), Article 2(7) of the KSC Act

KSC **Notify the significant incident (incident notification within 72 h)**

The notification describes the impact of the incident on the service, its causes and course, and the preventive and remedial action taken. The addressee and the channel are the same as for the early warning. The 72 h deadline runs from detection, not from the early warning. You pass on what you know at the time of notification and complete it while handling the incident.

by Tue 17 Nov 2026, 08:33 Polish time

Legal basis: Article 11(1)(4a) of the KSC Act, Article 12(3) of the KSC Act, Article 12(5) of the KSC Act

GDPR **Communicate the breach to the data subjects — preliminarily, the risk is high**

Your answers indicate that the breach is likely to result in a high risk to individuals. Explain in plain language what happened and what the consequences may be. Add what you are doing and what the individuals can do themselves, e.g. block their PESEL number or change passwords. Give the contact details of the DPO or another contact point. Communication is not required where, before the event, the data was protected so that it is unintelligible to unauthorised persons (e.g. encrypted with the key kept safe), or where measures taken afterwards ensure that the high risk is no longer likely to materialise (points (a) and (b) of Article 34(3)). Encryption of files by an attacker is not such a safeguard. Where communicating with each person would involve disproportionate effort, a public communication or an equally effective measure takes its place. The preliminary assessment follows from the type of data. Communication is not required if the measures taken after the event have made the high risk no longer likely (Article 34(3)(b) GDPR) — this is decided by the controller (with the DPO, if one has been designated); the President of UODO may require the communication or decide that the exception applies (Article 34(4) GDPR).

without undue delay — do not wait for 72 h to pass

Legal basis: Article 34(1) GDPR, Article 34(2) GDPR, points (a)–(c) of Article 34(3) GDPR

GDPR **Notify the breach to the President of UODO (the Polish data protection authority)**

Notify without undue delay and, where feasible, within 72 h of becoming aware of the breach. The notification describes the nature of the breach, its likely consequences and the measures taken. It also gives the contact details of the DPO or another contact point. You can complete the information later — it is better to notify with incomplete information than late. If you notify after the deadline, attach the reasons for the delay. An essential or important entity may also notify the breach through S46.

by Tue 17 Nov 2026, 10:33 Polish time

Legal basis: Article 33(1) GDPR, Article 33(3) GDPR, Article 33(4) GDPR, Article 46(1)(7) of the KSC Act, UODO statement of 3 November 2026 (recommendation)

GDPR **Record the breach in the breach register**

Describe every breach, including those not notified. Record the facts, the effects and the remedial action taken. The EDPB recommends also recording the reasoning for the decision, especially when you do not notify the breach. The documentation must enable the President of UODO to verify that you comply with Article 33.

on an ongoing basis

Legal basis: Article 33(5) GDPR, EDPB Guidelines 9/2022, paragraph 125 (guidelines, not a legal provision)

KSC **Submit a final report**

You submit the report within one month of the day on which you notify the significant incident. If handling is still ongoing, by that deadline you submit a progress report, and the final report within one month of completing the handling. You submit an interim report only at the request of the CSIRT.

one month from the day of the incident notification

Legal basis: points 4b and 4c of Article 11(1) of the KSC Act, paragraphs 1 and 2 of Article 12b of the KSC Act, Article 12a of the KSC Act

KSC **Inform the users of your services**

Where a significant incident adversely affects your services, you inform their users about it. The Act sets no deadline or form. I recommend doing this without delay and keeping the text of the message.

without delay — the Act sets no deadline

Legal basis: Article 11(2b) of the KSC Act

TO BE ESTABLISHED AND RECOMMENDATIONS

KSC **Competent CSIRT: CSIRT NASK**

According to your answer, CSIRT NASK is competent. The Act assigns to it essential and important entities not covered by CSIRT MON or CSIRT GOV. The exception is an incident in systems included in the critical infrastructure list — then CSIRT GOV is competent. Confirm this in your entry in the list of essential and important entities. Until the date of the statement on the operational capability of the sectoral CSIRT, notifications are accepted by the competent CSIRT MON, NASK or GOV. CSIRT INFRASTRUKTURA (transport, drinking water, waste water) was established by an order of the Minister of Infrastructure of 22 June 2026, and CSIRT Cyfra (digital infrastructure) by an order of the Minister of Digital Affairs of 30 June 2026. As at 11 November 2026, no statement on their operational capability had been found. For notifications under Article 11, the Act designates S46. If you cannot notify through S46, you notify in the manner that the competent CSIRT has set out in a statement in the Public Information Bulletin. Keep proof of the notification.

check before notifying

Legal basis: Article 26(6)(1)(j) of the KSC Act, Article 26(7)(6) of the KSC Act, points 21 and 22 of Article 7(2) of the KSC Act, Article 44(1) of the Act of 23 January 2026 (Journal of Laws 2026, item 252)

Law enforcement **Consider reporting to the police or the public prosecutor**

Keep the evidence. If a crime has been committed, consider reporting it to the police or the public prosecutor and keep the confirmation. Where a significant incident meets the statutory elements of a criminal offence, the CSIRT, in its response to the early warning, provides information on how to report it to law enforcement.

no deadline

Legal basis: second sentence of Article 12(2) of the KSC Act, LabLogic recommendation — good practice, not a legal provision

How this result was reached

- Role in relation to the data (according to your answers): controller.
- GDPR, risk to individuals (preliminary assessment): high — data: contact details, PESEL number or ID card, financial; number of people: 11–1,000. The tool's criteria are precautionary. The assessment is made by the controller (Article 33(1) and Article 34(1) GDPR).
- KSC, status: essential entity (according to your answers).
- KSC, significant incident (preliminary assessment): yes — the service was down for several hours or longer, or is still down (definition in Article 2(7) of the KSC Act; the tool does not calculate sectoral thresholds).
- KSC, whether the notification obligation already binds you: yes — an operator of essential services from before 3 April 2026 notifies from 3 October 2026 (Article 33(4) of the Act of 23 January 2026).
- KSC, addressee of the notification: CSIRT NASK (according to your answers). The addressee of the notification is set by points 4 and 4a of Article 11(1) of the KSC Act (the sectoral CSIRT), and, until the date of the statement on its operational capability, Article 44(1) of the Act of 23 January 2026 (CSIRT MON, CSIRT NASK or CSIRT GOV). The competence of CSIRT MON, CSIRT NASK or CSIRT GOV to coordinate incident handling follows from paragraphs 5–7 of Article 26 of the KSC Act, and your entry in the list of essential and important entities names the competent CSIRT (points 21 and 22 of Article 7(2) of the KSC Act).
- Questions without an answer or answered “I don't know”: losses and harm, possible effects. For these, the result takes the more cautious option.

What the notification contains

A summary of the statutory requirements; the full wording is in the “Legal bases” part. The authority's form may require more. Tick what you already have. The deadline runs even if you do not have all the information.

Notification to the President of UODO — Article 33(3) GDPR

- ☐ the nature of the breach, where possible with the categories and approximate number of data subjects and of personal data records concerned
- ☐ the name and contact details of the DPO or another contact point
- ☐ the likely consequences of the breach
- ☐ the measures taken or proposed, including those mitigating its adverse effects

Communication to the data subjects — Article 34(2) GDPR

- ☐ the nature of the breach, described in clear and plain language
- ☐ the name and contact details of the DPO or another contact point
- ☐ the likely consequences of the breach
- ☐ the measures taken or proposed, including those mitigating its adverse effects

Early warning (KSC) — Article 12(1) of the KSC Act

- ☐ the entity's details: business name, register number, registered office and address
- ☐ the person making the notification: name, surname, phone and work email
- ☐ the person authorised to provide explanations: name, surname, phone and work email
- ☐ the moment the incident occurred and was detected, and its duration
- ☐ whether the incident was caused by unlawful action or action in bad faith — if this can be assessed
- ☐ whether the incident affects other EU Member States
- ☐ marking of information constituting legally protected secrets, including trade secrets (Article 12(8))

Notification of a significant incident (KSC) — Article 12(3) of the KSC Act

- ☐ impact on the service: which service, number of users, geographical reach and impact on other entities
- ☐ causes, course and likely effects on the systems or services
- ☐ preventive action taken
- ☐ remedial action taken
- ☐ an update of the early warning information, if it has changed
- ☐ marking of information constituting legally protected secrets, including trade secrets (Article 12(8))

Final report (KSC) — Article 12a of the KSC Act

- ☐ a detailed description of the incident, including the disruption and damage
- ☐ the type of threat or the likely cause
- ☐ risk mitigation measures applied and being implemented
- ☐ cross-border effects, if any

Incident card

Type	Encrypted files, ransom demand
Detected	Sat 14 Nov 2026, 08:33 Polish time
Became aware of the data breach	Sat 14 Nov 2026, 10:33 Polish time
Role in relation to the data	controller
KSC status according to the answers	essential entity
Telecommunications / critical entity	no
Operator of essential services before 3 April 2026	yes
Essential or important entity since	not applicable — former operator of essential services, an essential entity since 3 April 2026
Competent CSIRT according to the answers	CSIRT NASK
Financial sector	no
Personal data	yes (contact details, PESEL number or ID card, financial)
Number of people	11–1,000
Data encrypted before the event, key safe	not applicable to this type of event
Impact on the service	the service is still down or degraded
Financial losses or harm to others	unknown
May still cause serious effects	not given
Deliberate action	yes

To complete in your documentation

The tool does not ask for the organisation's name. Complete these fields yourself before the plan goes into the case file.

Organisation	_____
Who noticed the event	_____
When the incident occurred (if earlier than it was detected)	_____
Who became aware of the data breach, and when	_____
Who decided to notify or not to notify, when and why	_____
Notification number in S46 / with the President of UODO	_____
Plan version (sequential number; supersedes the plan dated ...)	_____
Prepared by (name, surname, date)	_____
Verified by — DPO or adviser (date, changes compared with the tool's result)	_____
Approved by (name, surname, date, signature)	_____

HOW TO USE THE PLAN

The plan was created on your device

It was created in the browser from the answers given in the questionnaire and has not been sent anywhere. Keep it as incident documentation, because it describes an event in your organisation. When you learn something new, go back to the tool at incydent.lablogic.pl, change the answers and download a new version.

Legal bases — wording of the provisions

All times in the plan are Polish time (CET/CEST).

Article 11(1)(4) of the KSC Act

"submit an early warning of a significant incident without delay, no later than 24 hours after its detection, to the competent sectoral CSIRT"

Unofficial translation — only the Polish text is legally binding.
Original (Polish): „zgłasza wczesne ostrzeżenie o incydencie poważnym niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego"

Article 11(2) of the KSC Act

"The early warning [...] shall be transmitted by means of the ICT system referred to in Article 46(1)."

Unofficial translation — only the Polish text is legally binding.
Original (Polish): „Wczesne ostrzeżenie [...] są przekazywane za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1."

Article 12(1) of the KSC Act

"The early warning referred to in Article 11(1)(4) shall contain: 1) the details of the notifying entity […]; 4) an indication of the moment of occurrence and of detection of the significant incident and of its duration; 5) an indication of whether the significant incident was caused by unlawful action or by action in bad faith, if such an assessment is possible; 6) a determination of whether the incident affects other Member States of the European Union"

Unofficial translation — only the Polish text is legally binding.
Original (Polish): „Wczesne ostrzeżenie, o którym mowa w art. 11 ust. 1 pkt 4, zawiera: 1) dane podmiotu zgłaszającego […]; 4) wskazanie momentu wystąpienia i wykrycia incydentu poważnego oraz czas jego trwania; 5) wskazanie, czy incydent poważny został wywołany działaniem bezprawnym lub działaniem w złej wierze, jeżeli możliwe jest dokonanie takiej oceny; 6) określenie, czy incydent dotyczy innych państw członkowskich Unii Europejskiej"

Article 12(2) of the KSC Act

"The early warning referred to in Article 11(1)(4) may contain a request for guidance on measures that may be implemented to mitigate the effects of the significant incident or for additional technical support in handling the incident. The sectoral CSIRT shall, within 24 hours at the latest, provide the notifying entity with guidance on the implementation of measures or provide additional technical support […]"

Unofficial translation — only the Polish text is legally binding.
Original (Polish): „Wczesne ostrzeżenie, o którym mowa w art. 11 ust. 1 pkt 4, może zawierać wniosek o wskazanie wytycznych dotyczących możliwych do wdrożenia środków ograniczających skutki incydentu poważnego lub o dodatkowe wsparcie techniczne przy obsłudze incydentu. CSIRT sektorowy nie później niż w ciągu 24 godzin przekazuje podmiotowi zgłaszającemu wytyczne dotyczące wdrożenia środków lub udziela dodatkowego wsparcia technicznego […]"

Article 44(1) of the Act of 23 January 2026 (Journal of Laws 2026, item 252)

"Until the date of issue of the statement referred to in Article 42(2) […], essential entities or important entities shall notify significant incidents in accordance with Articles 11–12b […] to the competent CSIRT MON, CSIRT NASK or CSIRT GOV."

Unofficial translation — only the Polish text is legally binding.
Original (Polish): „Do dnia wydania komunikatu, o którym mowa w art. 42 ust. 2 […], podmioty kluczowe lub podmioty ważne zgłaszają incydenty poważne zgodnie z art. 11–12b […] do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV."

Article 2(7) of the KSC Act

"an incident which causes or may cause a serious degradation in the quality or an interruption in the continuity of the provision of a service by an essential entity or an important entity, financial losses for that entity, or affects other natural persons, legal persons or organisational units without legal personality by causing serious material or non-material damage"

Unofficial translation — only the Polish text is legally binding.
Original (Polish): „incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi przez podmiot kluczowy lub podmiot ważny, straty finansowe dla tego podmiotu lub wpływa na inne osoby fizyczne, osoby prawne, jednostki organizacyjne nieposiadające osobowości prawnej przez wywołanie poważnej szkody materialnej lub niematerialnej"

Article 11(1)(4a) of the KSC Act

"notify the significant incident without delay, no later than 72 hours after its detection, to the competent sectoral CSIRT"

Unofficial translation — only the Polish text is legally binding.
Original (Polish): „zgłasza incydent poważny niezwłocznie, nie później niż w ciągu 72 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego"

Article 12(3) of the KSC Act

"The notification referred to in Article 11(1)(4a) shall contain: 1) a description of the impact of the significant incident on the provision of the service […]; 2) a description of the causes of that incident, the way in which it unfolded and its likely effects on the information systems or the services provided; 3) information on the preventive action taken; 4) information on the remedial action taken; 5) an update of the information referred to in paragraph 1, if it has changed"

Unofficial translation — only the Polish text is legally binding.
Original (Polish): „Zgłoszenie, o którym mowa w art. 11 ust. 1 pkt 4a, zawiera: 1) opis wpływu incydentu poważnego na świadczenie usługi […]; 2) opis przyczyn tego incydentu, sposób jego przebiegu oraz prawdopodobne skutki oddziaływania na systemy informacyjne lub świadczone usługi; 3) informacje o podjętych działaniach zapobiegawczych; 4) informacje o podjętych działaniach naprawczych; 5) aktualizację informacji, o których mowa w ust. 1, jeżeli nastąpiła ich zmiana"

Article 12(5) of the KSC Act

"The essential entity or important entity shall provide the information known to it at the time of making the notification referred to in Article 11(1)(4a), and shall supplement it in the course of handling the significant incident."

Unofficial translation — only the Polish text is legally binding.
Original (Polish): „Podmiot kluczowy lub podmiot ważny przekazuje informacje znane mu w chwili dokonywania zgłoszenia, o którym mowa w art. 11 ust. 1 pkt 4a, które uzupełnia w trakcie obsługi incydentu poważnego."

Article 34(1) GDPR

"When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."

Article 34(2) GDPR

"shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3)"

points (a)–(c) of Article 34(3) GDPR

"The communication to the data subject [...] shall not be required [...]: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk [...] is no longer likely to materialise; (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication [...]"

Article 33(1) GDPR

"the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority [...], unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."

Article 33(3) GDPR

"The notification referred to in paragraph 1 shall at least: (a) describe the nature of the personal data breach [...]; (b) communicate the name and contact details of the data protection officer or other contact point [...]; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach [...]"

Article 33(4) GDPR

"Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay."

Article 46(1)(7) of the KSC Act

"making the notification of a personal data breach referred to in Article 33 of Regulation 2016/679 [...] by essential entities or important entities"

Unofficial translation — only the Polish text is legally binding.
Original (Polish): „dokonywanie zgłoszenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 rozporządzenia 2016/679 [...], przez podmioty kluczowe lub podmioty ważne"

Article 33(5) GDPR

"The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article."

points 4b and 4c of Article 11(1) of the KSC Act

"provide, at the request of the competent sectoral CSIRT, an interim report [...]; provide [...] a final report on the handling of the significant incident, no later than one month after the day of the notification referred to in point 4a"

Unofficial translation — only the Polish text is legally binding.
Original (Polish): „przekazuje, na wniosek właściwego CSIRT sektorowego, sprawozdanie okresowe [...]; przekazuje [...] sprawozdanie końcowe z obsługi incydentu poważnego, nie później niż w ciągu miesiąca od dnia zgłoszenia, o którym mowa w pkt 4a"

paragraphs 1 and 2 of Article 12b of the KSC Act

"Where the handling of the significant incident has not been completed by the deadline for submitting the final report [...] shall provide [...] a progress report on the handling of that incident [...] a final report no later than one month after the completion of the handling of the significant incident."

Unofficial translation — only the Polish text is legally binding.
Original (Polish): „W przypadku gdy obsługa incydentu poważnego nie zakończyła się w terminie składania sprawozdania końcowego [...] przekazuje [...] sprawozdanie z postępu obsługi tego incydentu [...] sprawozdanie końcowe nie później niż w ciągu miesiąca od zakończenia obsługi incydentu poważnego."

Article 12a of the KSC Act

"The final report referred to in Article 11(1)(4c) shall contain: 1) a detailed description of the significant incident, including the disruption and damage caused; 2) the type of threat or the cause that was likely the source of the incident; 3) the risk mitigation measures applied and being implemented; 4) the cross-border effects of the incident, if any"

Unofficial translation — only the Polish text is legally binding.
Original (Polish): „Sprawozdanie końcowe, o którym mowa w art. 11 ust. 1 pkt 4c, zawiera: 1) szczegółowy opis incydentu poważnego, w tym spowodowane zakłócenia i szkody; 2) rodzaj zagrożenia lub przyczynę, która prawdopodobnie była źródłem incydentu; 3) zastosowane i wdrażane środki ograniczające ryzyko; 4) transgraniczne skutki incydentu, jeżeli wystąpiły"

Article 11(2b) of the KSC Act

"An essential entity or an important entity shall inform the users of its services of a significant incident if it adversely affects the provision of those services."

Unofficial translation — only the Polish text is legally binding.
Original (Polish): „Podmiot kluczowy lub podmiot ważny informuje użytkowników swoich usług o incydencie poważnym, jeżeli ma on niekorzystny wpływ na świadczenie tych usług."

Article 26(6)(1)(j) of the KSC Act

"essential entities or important entities, with the exception of those listed in paragraphs 5 and 7"

Unofficial translation — only the Polish text is legally binding.
Original (Polish): „podmioty kluczowe lub podmioty ważne, z wyjątkiem wymienionych w ust. 5 i 7"

Article 26(7)(6) of the KSC Act

"the entities referred to in paragraph 6, if the incident concerns ICT systems or ICT networks included in the list"

Unofficial translation — only the Polish text is legally binding.
Original (Polish): „podmioty, o których mowa w ust. 6, jeżeli incydent dotyczy systemów teleinformatycznych lub sieci teleinformatycznych objętych wykazem"

points 21 and 22 of Article 7(2) of the KSC Act

"The list shall contain: […] 21) an indication of the sectoral CSIRT competent for the essential entity or important entity; 22) an indication of CSIRT MON, CSIRT NASK or CSIRT GOV competent for the essential entity or important entity"

Unofficial translation — only the Polish text is legally binding.
Original (Polish): „Wykaz zawiera: […] 21) wskazanie CSIRT sektorowego właściwego dla podmiotu kluczowego lub podmiotu ważnego; 22) wskazanie CSIRT MON, CSIRT NASK lub CSIRT GOV właściwego dla podmiotu kluczowego lub podmiotu ważnego"

second sentence of Article 12(2) of the KSC Act

"and, in the case of a significant incident that fulfils the statutory elements of a criminal offence, also information on how to report it to law enforcement authorities"

Unofficial translation — only the Polish text is legally binding.
Original (Polish): „a w przypadku incydentu poważnego wyczerpującego znamiona przestępstwa również informacje o sposobie zgłoszenia organom ścigania"

Acts and materials

- Regulation (EU) 2016/679 (GDPR)
  OJ L 119, 4.5.2016
  eur-lex.europa.eu/eli/reg/2016/679/oj/eng
- Act of 5 July 2018 on the national cybersecurity system (KSC Act)
  consolidated text by the Chancellery of the Sejm: Journal of Laws 2026, items 20, 252, 815, 1003
  isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560
- Act of 23 January 2026 amending the KSC Act and certain other acts
  Journal of Laws 2026, item 252
  isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20260000252
- Statement of the President of UODO of 3 November 2026 "We recommend notifying a personal data breach through S46"
  uodo.gov.pl/pl/138/4650
- EDPB Guidelines 9/2022 on personal data breach notification under GDPR, version 2.0
  www.edpb.europa.eu/documents/guideline/guidelines-92022-on-personal-data-breach-notification-under-gdpr_en

LABLOGIC · GDPR AND NIS2/KSC

If you need support

Michał Rutkowski, data protection officer and NIS2/KSC adviser. I help companies and institutions get through an incident and then put their data protection and cybersecurity in order.

Incident and data breach response

Assessment of the event, notifications to the CSIRT and to the President of UODO, communication to individuals, the breach register and the final report. I start with a phone call.
lablogic.pl/en/incident-response

External data protection officer

Acting as your DPO on an ongoing basis: day-to-day advice, registers, data subject requests and contact with the President of UODO.
lablogic.pl/en/external-dpo

NIS2 and KSC implementation

Establishing the organisation's status, the application for entry in the list, the information security management system and the incident handling procedure.
lablogic.pl/en/nis2-ksc

Training and exercises

Training for management and staff, and incident handling exercises based on a scenario similar to yours.
lablogic.pl/en/training

Before the call, prepare

- This plan and the times of detection and of becoming aware of the breach.
- A list of the systems and services that are not working.
- Information on whether the backups are intact and disconnected from the network.
- Contact details of a person who can take decisions in the organisation.

Call or write

+48 504 920 875

m.rutkowski@lablogic.pl · form: incydent.lablogic.pl/en/ · lablogic.pl

I answer the phone on working days, 8–16 Polish time. Outside these hours, leave your number in the form at incydent.lablogic.pl — I will call back on the next working day. The first call is free of charge and without obligation.

Preliminary assessment from the LabLogic tool (version 1.22 of 14 Nov 2026, law as at 11 Nov 2026). It is not a legal opinion. The result depends on the answers given in the questionnaire. Deadlines are counted from the times given in the questionnaire.
LabLogic Consulting Michał Rutkowski · ul. Wolności 15/6, 81-327 Gdynia, Poland · NIP (tax ID) 958-097-21-14 · REGON 193029560