CSIRT NASK’s Privacy Policy

CSIRT NASK is the Computer Security Incident Response Team, which operates on the national level and is run by Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy (NASK) with its registered office in Warsaw.

CSIRT NASK’s competencies and duties are set out in the Act on the National Cybersecurity System of 13 August 2018 (Dz.U. [Journal of Laws] 2018, item 1560), hereinafter referred to as ANCS.

1. Policy objective

This Privacy Policy contains basic information about data processing performed in connection with the operations of CSIRT NASK. We take all actions on the basis of legal regulations in force, in particular ANCS provisions and regulations concerning the protection of personal data. When processing your data, we make our best efforts to do it fairly and transparently, and protect your privacy.

2. Processing of personal data

The controller of your personal data processed by CSIRT NASK is Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy (NASK) with its registered office in Warsaw, ul. Kolska 12, 01-045 Warsaw.

NASK appointed a Data Protection Officer, who can be contacted at the address: inspektorochronydanych@nask.pl.

In connection with the performed tasks, CSIRT NASK can process personal data obtained in connection with cybersecurity incidents and threats, for the purposes stemming from CSIRT NASK’s task, which include in particular:

- to monitor cybersecurity threats and incidents at the national level;
- to assess the risk associated with the revealed cybersecurity threat and existing incidents;
- to share information on incidents and risks with actors in the national cybersecurity system;
- to issue updates on identified threats to cybersecurity;
- to respond to reported incidents;
- to classify incidents, including major incidents and material incidents, as critical incidents, and
- to co-ordinate the handling of critical incidents;
- to share with other states, including European Union Member States, and to receive from such states information on major incidents and material incidents concerning two or more Member States, and to share with the Single Contact Point the report of a major or material incident concerning two or more European Union Member States;
- to provide resources for analysis and R&D;
- to enable the reporting of incidents and to share and handle the means of communications, which help make such reports;

- to create and make available tools for voluntary co-operation and exchange of information on cybersecurity threats and incidents;
- to receive reports concerning illegal content in the Internet, in particular content related to sexual abuse of children.

CSIRT NASK processes personal data exclusively on in the basis of:

1. its obligation under the laws, in particular the ANCS;
2. data subject's prior voluntary consent for the processing of his/her personal data (e.g. when registering for the SECURE conference);
3. agreements signed with trusted partners and counterparties with respect to notification of threats, vulnerabilities and incidents;
4. legitimate interest pursued by CSIRT NASK or a third party (e.g. for scientific or historical research as well as for statistical purposes, in connection with the determination, pursue, or defence against claims).

CSIRT NASK process personal data only to the extent necessary to achieve the purpose, for which the data was collected.

CSIRT NASK declares that CSIRT NASK's websites function with the highest due diligence, good technical principles and principles of industrial professionalism as well as in compliance with applicable laws, in particular those which protect the privacy of Internet site users.

In some cases, when reporting an incident with the use of the form at www.incydent.cert.pl, it is obligatory under the ANCS to provide his/her name and surname, phone number and e-mail address for the reporting person and for the person authorised to provide explanations.

In other cases, when using the incident report form at www.incydent.cert.pl or www.dyzurnet.pl, the data subject can make a free decision whether to provide or not to provide his/her data, however the provision of personal data may be required in a situation where the data subject is interested in receiving information regarding the handling of the incident reported on site www.incydent.cert.pl.

3. Categories of personal data

CSIRT NASK processes personal data obtained in connection with cybersecurity incidents and threats:

1. concerning users of IT systems and users of telecommunications terminal devices;
2. concerning telecommunications terminal devices within the meaning of Article 2(43) of the Polish Telecommunication Law of 16 July 2004;
3. collected by key service operators and digital service providers in connection with the provision of services;
4. collected by public entities in connection with their performance of public tasks;
5. concerning the entities reporting the incident.

4. Time limit for the storage of personal data

CSIRT NASK processes personal data for a period not longer than necessary for the purposes, for which such data is processed, in particular to handle an incident.

Personal data obtained in connection with cybersecurity incidents and threats, necessary for CSIRT NASK to carry out its tasks, is removed or anonymised within 5 years of the end of handling of the incident, to which the data pertains.

5. Personal data sharing

Personal data obtained in connection with cybersecurity incidents and threats can be shares with other CSIRTS at the national level i.e. CSIRT MON and CSIRT GOV, and with sector cybersecurity teams, for the purpose of performance of their tasks set out by laws, in particular the ANCS.

6. Data subjects' rights

The processing of personal data obtained in connection with cybersecurity incidents and threats, listed in item 3 of this Policy, shall not require carrying out the duties referred to in Articles 15, 16, 18(1)(a), 18(1)(d) and 19, second sentence, of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016. on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: "GDPR"), if this were to prevent the performance of CSIRT NASK's tasks set out in the ANCS.

When the conditions set out in the precedent sentence do not apply, the data subject whose data is processed by CSIRT NASK has the right to demand: access to his/her data, rectification of his/her data, restricted use of his/her data and erasure of his/her data, and the right to transfer the to another controller; when the data is processed on the basis of a consent - the right to withdraw the consent given; this will not affect the lawfulness of any data processing done on the basis of that consent before it was revoked.

Such data subject has also the right to object against the processing of his/her personal data and the right to lodge a complaint with the supervisory authority for personal data protection.

7. Means of security in the processing of personal data

When processing personal data, CSIRT NSK performs a risk analysis, applies means of protection against malware and access control mechanism, and develops procedures for secure data exchange.