

GDPR Privacy Notice for Persons Reporting a Vulnerability, Cyber Threat or Incident

1. Data Controller

The controller of your personal data is ACTION S.A., with its registered office in Zamienie, ul. Dawidowska 10, 05-500 Piaseczno, Poland, entered in the Register of Entrepreneurs of the National Court Register under KRS number 0000214038, NIP 527-11-07-221, REGON 011909816.

2. Contact for Data Protection Matters

For matters concerning the processing of personal data, you may contact the Data Protection Officer, Waldemar Gełzakowski, at iod@action.pl or by post at the Controller's registered office, marked "Data Protection Officer".

Security reports themselves should be submitted using the reporting form at <https://www.action.pl/pl/kontakt/zgloszenie-podatnosci> or by email to safety@action.pl. These are separate channels handled by the security team.

3. Purposes of Processing and Legal Bases

Purpose	Legal basis
Receipt of a report, technical verification, follow-up contact and requests for further details	Article 6(1)(f) GDPR— the Controller's legitimate interest in handling the report and ensuring the security of networks, products and services (see Recital 49 GDPR)
Remediation of vulnerabilities, preparation and provision of security updates, and informing users	Article 6(1)(c) GDPR—legal obligation arising from Articles 13 and 14 of Regulation (EU) 2024/2847 (Cyber Resilience Act)
Reporting an actively exploited vulnerability or a serious incident to CSIRT NASK and ENISA	Article 6(1)(c) GDPR—Article 14 of Regulation (EU) 2024/2847
Incident handling and reporting a serious incident to the competent CSIRT team	Article 6(1)(c) GDPR—Article 11 of the Act of 5 July 2018 on the National Cybersecurity System
Providing information to the manufacturer of the component or software in which a vulnerability exists (coordinated vulnerability disclosure)	Article 6(1)(f) GDPR—the legitimate interest in ensuring that the vulnerability is remedied at its source
Maintaining records of reports, incidents and remedial actions, and demonstrating compliance with regulations	Article 6(1)(c) GDPR—Article 10 of the Act on the National Cybersecurity System and Article 31 of Regulation (EU) 2024/2847; Article 6(1)(f) GDPR— legitimate interest in demonstrating due diligence
Naming the person reporting a vulnerability, by their full name or pseudonym, in published information about the vulnerability	Article 6(1)(a) GDPR—your consent, which you may withdraw at any time
Establishment, exercise or defence of legal claims	Article 6(1)(f) GDPR—the Controller's legitimate interest

Purpose	Legal basis
Protecting the reporting form against abuse and automated submissions (reCAPTCHA mechanism)	Article 6(1)(f) GDPR—the Controller’s legitimate interest in ensuring the proper functioning of the form and protecting it against abuse

4. Is Providing Data Mandatory?

No. You may submit a report anonymously—we will accept and handle it in the same way as any other report. Providing contact details is voluntary and is only necessary if you wish to receive a response or if we need to ask you for further details about the report. Without them, we will not be able to contact you.

5. Recipients of Data

Your data may be disclosed to:

- the CSIRT NASK team and, in cases specified by law, CSIRT MON or CSIRT GOV;
- the European Union Agency for Cybersecurity (ENISA), via the single reporting platform, where the report concerns an actively exploited vulnerability;
- the competent cybersecurity authority and other public authorities authorised by law, including law enforcement authorities;
- manufacturers and suppliers of components, software or services affected by the reported vulnerability, to the extent necessary to remediate it;
- entities belonging to the ACTION Capital Group;
- IT service providers acting on our behalf (hosting, email, reporting systems);
- legal advisers, auditors and consultancy service providers, to the extent necessary to achieve the stated purposes;
- the provider of the reCAPTCHA mechanism protecting the reporting form, to the extent of the data processed by that mechanism.

Reports forwarded to authorities and manufacturers primarily contain a technical description of the problem. We disclose your contact details only where necessary—for example, where the recipient needs them to investigate the matter further.

6. Transfers of Data Outside the European Economic Area

The CSIRT teams and ENISA operate within the European Union. However, if the reported vulnerability concerns a component, software or service supplied by a manufacturer established outside the EEA, sharing information about the vulnerability may involve transferring data to a third country. Such transfers are based on an European Commission adequacy decision (Article 45 GDPR) or standard contractual clauses approved by the Commission (Article 46(2)(c) GDPR). You may obtain information about the safeguards applied and a copy of them by emailing iod@action.pl.

A separate basis applies to data transfers associated with the reCAPTCHA mechanism that protects the reporting form. Technical data processed by this mechanism—in particular, the IP address and information about how the website is used—may be transferred outside the European Economic Area. Such transfers are based on a European Commission implementing decision finding an adequate level of protection (Article 45 GDPR) or standard contractual clauses (Article 46(2)(c) GDPR). Detailed information about the safeguards is available upon request sent to iod@action.pl.

7. Data Retention Period

We do not retain data for longer than is necessary for the purposes set out in Section 3. Cybersecurity legislation does not establish a single retention period for reports; therefore, the criteria used to determine retention periods are set out below (Article 13(2)(a) GDPR).

Category of data	Criteria for determining the retention period
Report content and correspondence with the person submitting the report	Until the report has been handled and the effectiveness of remedial actions has been confirmed
Report included in documentation concerning the security of an information system	Under Article 10(7) of the Act on the National Cybersecurity System, documentation must be retained for at least 2 years from the date on which the system is withdrawn from use or the service provision ends
Technical description of a vulnerability included in product documentation	For the duration of product support; contact details of the person submitting the report are not included in product documentation
Data processed on the basis of consent (identification in a publication)	Until consent is withdrawn
Data necessary for the establishment, exercise or defence of legal claims	Until the limitation period for claims expires
Technical data processed by the reCAPTCHA mechanism	For the period determined by the rules applied by the provider of this mechanism; the Controller does not store this data in a separate dataset

Reports forwarded to authorities—CSIRT NASK or ENISA—are retained by those authorities in accordance with their own rules, independently of the above.

8. Your Rights

You have the right to:

- access your data and obtain a copy;
- rectify (correct) your data;
- erase your data;
- restrict processing;
- object to processing based on the Controller's legitimate interests, on grounds relating to your particular situation (Article 21(1) GDPR);
- data portability, in respect of data processed on the basis of consent;
- withdraw your consent at any time, without affecting the lawfulness of processing carried out before its withdrawal;
- lodge a complaint with the President of the Personal Data Protection Office, ul. Stanisława Moniuszki 1A, 00-014 Warsaw, Poland.

Where we process data to fulfil obligations arising from cybersecurity legislation, it may not be possible to comply with a request for erasure or an objection.

9. Automated Decision-Making

Reports may be subject to preliminary automated classification; however, this does not result in a decision based solely on automated processing that produces legal effects concerning you or similarly significantly affects you. We do not use profiling.

10. Personal Data of Other Individuals Included in a Report

Please do not include other individuals' personal data in your report—including screenshots, logs and files containing such data—unless this is necessary to describe the problem. If a report contains third parties' data, we will process it solely to handle the report and fulfil the obligations specified in Section 3. The source of this data is the report submitted to us (Article 14 GDPR).

11. Protection of the Reporting Form

The reporting form is protected by the reCAPTCHA mechanism, which distinguishes reports submitted by people from those sent automatically. This mechanism processes technical data about your device and how you use the website, including your IP address. We do not use this data to identify the person submitting the report or to assess the content of the report, and its processing does not affect the ability to submit a report anonymously.