Klauzula informacyjna RODO dla zgłaszających podatność, cyberzagrożenie, incydent

1. Administrator danych

Administratorem Twoich danych osobowych jest ACTION S.A. z siedzibą w Zamieniu, ul. Dawidowska 10, 05-500 Piaseczno, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS 0000214038, NIP 527-11-07-221, REGON 011909816.

2. Kontakt w sprawach ochrony danych

W sprawach dotyczących przetwarzania danych osobowych możesz skontaktować się z Inspektorem Ochrony Danych, którym jest Waldemar Gełzakowski: iod@action.pl lub listownie na adres siedziby Administratora z dopiskiem „Inspektor Ochrony Danych".
Samo zgłoszenie bezpieczeństwa kierujesz za pośrednictwem formularza zgłoszeniowego na stronie https://www.action.pl/pl/kontakt/zgloszenie-podatnosci lub na adres safety@action.pl — to odrębne kanały, obsługiwane przez zespół bezpieczeństwa.

3. Cele przetwarzania i podstawy prawne

Cel	Podstawa prawna
Przyjęcie zgłoszenia, jego weryfikacja techniczna, kontakt zwrotny i dopytanie o szczegóły	art. 6 ust. 1 lit. f RODO — prawnie uzasadniony interes Administratora polegający na obsłudze zgłoszenia oraz zapewnieniu bezpieczeństwa sieci, produktów i usług (por. motyw 49 RODO)
Usunięcie podatności, przygotowanie i udostępnienie aktualizacji zabezpieczeń, poinformowanie użytkowników	art. 6 ust. 1 lit. c RODO — obowiązek prawny wynikający z art. 13 i 14 rozporządzenia (UE) 2024/2847 (akt o cyberodporności)
Zgłoszenie aktywnie wykorzystywanej podatności lub poważnego incydentu do CSIRT NASK oraz ENISA	art. 6 ust. 1 lit. c RODO — art. 14 rozporządzenia (UE) 2024/2847
Obsługa incydentu i zgłoszenie incydentu poważnego do właściwego zespołu CSIRT	art. 6 ust. 1 lit. c RODO — art. 11 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa
Przekazanie informacji producentowi komponentu lub oprogramowania, w którym występuje podatność (skoordynowane ujawnianie podatności)	art. 6 ust. 1 lit. f RODO — prawnie uzasadniony interes polegający na doprowadzeniu do usunięcia podatności u jej źródła
Prowadzenie dokumentacji zgłoszeń, incydentów i działań naprawczych oraz wykazanie zgodności z przepisami	art. 6 ust. 1 lit. c RODO — art. 10 ustawy o krajowym systemie cyberbezpieczeństwa oraz art. 31 rozporządzenia (UE) 2024/2847; art. 6 ust. 1 lit. f RODO — interes w wykazaniu należytej staranności
Wskazanie imienia i nazwiska albo pseudonimu osoby zgłaszającej w publikowanej informacji o podatności	art. 6 ust. 1 lit. a RODO — Twoja zgoda, którą możesz wycofać w każdej chwili
Ustalenie, dochodzenie lub obrona roszczeń	art. 6 ust. 1 lit. f RODO — prawnie uzasadniony interes Administratora

Cel	Podstawa prawna
Zabezpieczenie formularza zgłoszeniowego przed nadużyciami i automatycznym wysyłaniem zgłoszeń (mechanizm reCAPTCHA)	art. 6 ust. 1 lit. f RODO — prawnie uzasadniony interes Administratora polegający na zapewnieniu prawidłowego działania formularza i ochronie przed nadużyciami

4. Czy podanie danych jest obowiązkowe

Nie. **Zgłoszenie możesz złożyć anonimowo** — przyjmiemy je i rozpatrzymy tak samo jak każde inne. Podanie danych kontaktowych jest dobrowolne i jest potrzebne wyłącznie wtedy, gdy chcesz otrzymać odpowiedź albo gdy będziemy musieli dopytać o szczegóły zgłoszenia. Bez nich nie będziemy mogli się z Tobą skontaktować.

5. Odbiorcy danych

Twoje dane mogą zostać przekazane:

- zespołowi CSIRT NASK, a w przypadkach określonych ustawą — CSIRT MON albo CSIRT GOV;
- Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) — za pośrednictwem jednolitej platformy zgłoszeniowej, gdy zgłoszenie dotyczy aktywnie wykorzystywanej podatności;
- organowi właściwemu do spraw cyberbezpieczeństwa oraz innym organom publicznym uprawnionym na podstawie przepisów prawa, w tym organom ścigania;
- producentom i dostawcom komponentów, oprogramowania lub usług, w których występuje zgłoszona podatność — w zakresie niezbędnym do jej usunięcia;
- podmiotom należącym do Grupy Kapitałowej ACTION;
- dostawcom usług IT działającym na nasze zlecenie (hosting, poczta elektroniczna, systemy obsługi zgłoszeń);
- doradcom prawnym, audytorom i podmiotom świadczącym usługi doradcze — w zakresie niezbędnym do realizacji wskazanych celów.
- dostawcy mechanizmu reCAPTCHA zabezpieczającego formularz zgłoszeniowy — w zakresie danych przetwarzanych przez ten mechanizm.

Zgłoszenie przekazywane organom i producentom obejmuje przede wszystkim opis techniczny problemu. Twoje dane kontaktowe przekazujemy tylko wtedy, gdy jest to niezbędne — na przykład gdy odbiorca potrzebuje ich do dalszego wyjaśnienia sprawy.

6. Przekazywanie danych poza Europejski Obszar Gospodarczy

Zespoły CSIRT oraz ENISA działają na terenie Unii Europejskiej. Jeżeli jednak zgłoszona podatność dotyczy komponentu, oprogramowania lub usługi producenta mającego siedzibę poza EOG, przekazanie informacji o podatności może wiązać się z przekazaniem danych do państwa trzeciego. Odbywa się to na podstawie decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony (art. 45 RODO) albo standardowych klauzul umownych zatwierdzonych przez Komisję (art. 46 ust. 2 lit. c RODO). Informację o zastosowanych zabezpieczeniach i ich kopię możesz uzyskać, pisząc na iod@action.pl.

Odrębną podstawę ma przekazanie danych związane z działaniem mechanizmu reCAPTCHA, który zabezpiecza formularz zgłoszeniowy. Dane techniczne przetwarzane przez ten mechanizm — w szczególności adres IP oraz informacje o sposobie korzystania ze strony — mogą być przekazywane poza Europejski Obszar Gospodarczy. Przekazanie odbywa się na podstawie decyzji wykonawczej Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony (art. 45 RODO) albo standardowych

klauzul umownych (art. 46 ust. 2 lit. c RODO). Szczegółowe informacje o zabezpieczeniach udostępniamy na wniosek skierowany na iod@action.pl.

7. Okres przechowywania danych

Nie przechowujemy danych dłużej, niż jest to niezbędne do celów wskazanych w pkt 3. Przepisy o cyberbezpieczeństwie nie wyznaczają jednego terminu przechowywania zgłoszeń, dlatego poniżej wskazujemy kryteria ustalania okresu przechowywania (art. 13 ust. 2 lit. a RODO).

Kategoria danych	Kryterium ustalenia okresu przechowywania
Treść zgłoszenia i korespondencja z osobą zgłaszającą	do zakończenia obsługi zgłoszenia i potwierdzenia skuteczności działań naprawczych
Zgłoszenie włączone do dokumentacji dotyczącej bezpieczeństwa systemu informacyjnego	zgodnie z art. 10 ust. 7 ustawy o krajowym systemie cyberbezpieczeństwa dokumentację przechowuje się nie krócej niż 2 lata od dnia jej wycofania z użytkowania lub zakończenia świadczenia usługi
Opis techniczny podatności włączony do dokumentacji produktu	przez okres wsparcia produktu; do dokumentacji produktu nie włączamy danych kontaktowych osoby zgłaszającej
Dane przetwarzane na podstawie zgody (wskazanie w publikacji)	do momentu wycofania zgody
Dane niezbędne do ustalenia, dochodzenia lub obrony roszczeń	do upływu terminu przedawnienia roszczeń
Dane techniczne przetwarzane przez mechanizm reCAPTCHA	przez okres wynikający z zasad stosowanych przez dostawcę tego mechanizmu; Administrator nie przechowuje tych danych w odrębnym zbiorze

Zgłoszenia przekazane organom — CSIRT NASK lub ENISA — są przechowywane przez te organy na zasadach przez nie określonych, niezależnie od powyższego.

8. Twoje prawa

Przysługuje Ci prawo do:

- dostępu do swoich danych oraz otrzymania ich kopii;
- sprostowania (poprawiania) danych;
- usunięcia danych;
- ograniczenia przetwarzania;
- wniesienia sprzeciwu wobec przetwarzania opartego na prawnie uzasadnionym interesie Administratora — z przyczyn związanych z Twoją szczególną sytuacją (art. 21 ust. 1 RODO);
- przenoszenia danych — w zakresie danych przetwarzanych na podstawie zgody;
- wycofania zgody w dowolnym momencie, bez wpływu na zgodność z prawem przetwarzania dokonanego przed jej wycofaniem;
- wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Stanisława Moniuszki 1A, 00-014 Warszawa.

W zakresie, w jakim przetwarzamy dane w celu wykonania obowiązków wynikających z przepisów o cyberbezpieczeństwie, uwzględnienie żądania usunięcia danych lub sprzeciwu może nie być możliwe.

9. Zautomatyzowane podejmowanie decyzji

Zgłoszenia mogą podlegać wstępnej, zautomatyzowanej klasyfikacji, jednak nie prowadzi to do decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu, która wywoływałaby wobec Ciebie skutki prawne lub w podobny sposób istotnie na Ciebie wpływała. Nie stosujemy profilowania.

10. Dane innych osób w treści zgłoszenia

Prosimy o **nieprzekazywanie w zgłoszeniu danych osobowych innych osób** — w tym zrzutów ekranu, logów i plików zawierających takie dane — jeżeli nie jest to niezbędne do opisania problemu. Jeżeli w zgłoszeniu znajdą się dane osób trzecich, będziemy je przetwarzać wyłącznie w celu obsługi zgłoszenia i wykonania obowiązków wskazanych w pkt 3; źródłem tych danych jest przekazane nam zgłoszenie (art. 14 RODO).

11. Zabezpieczenie formularza zgłoszeniowego

Formularz zgłoszeniowy jest zabezpieczony mechanizmem reCAPTCHA, który odróżnia zgłoszenia składane przez ludzi od wysyłanych automatycznie. Mechanizm ten przetwarza dane techniczne dotyczące Twojego urządzenia i sposobu korzystania ze strony, w tym adres IP. Nie wykorzystujemy tych danych do identyfikacji osoby zgłaszającej ani do oceny treści zgłoszenia, a ich przetwarzanie nie wpływa na możliwość złożenia zgłoszenia anonimowo.