Polityka prywatności CSIRT NASK

CSIRT NASK to Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy z siedzibą w Warszawie.

Kompetencje i obowiązki CSIRT NASK określa ustawa z dnia 13 sierpnia 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018, poz. 1560), zwana dalej: ustawą o k.s.c.

1. Cel Polityki

Niniejsza Polityka prywatności zawiera podstawowe informacje na temat przetwarzania danych, prowadzonego w związku z działaniem CSIRT NASK. Wszelkie działania podejmujemy w oparciu o obowiązujące przepisy prawa, w tym w szczególności przepisy ustawy o k.s.c. oraz o przepisy dotyczące ochrony danych osobowych. Przetwarzając Twoje dane dokładamy wszelkich starań, aby robić to rzetelnie i przejrzyście, chroniąc Twoją prywatność.

2. Przetwarzanie danych osobowych

Administratorem danych osobowych, przetwarzanych przez CSIRT NASK jest Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK) z siedzibą w Warszawie, ul. Kolska 12, 01-045 Warszawa.

NASK wyznaczył Inspektora Ochrony Danych, z którym możesz się skontaktować pod adresem: inspektorochronydanych@nask.pl.

W związku z realizowanymi zadaniami CSIRT NASK może przetwarzać dane osobowe pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa, w celach, które wynikają z zadań CSIRT NASK, a do których należą w szczególności:

- monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym;
- szacowanie ryzyka związanego z ujawnionym zagrożeniem cyberbezpieczeństwa oraz zaistniałymi incydentami;
- przekazywanie informacji dotyczących incydentów i ryzyk podmiotom krajowego systemu cyberbezpieczeństwa;
- wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa;
- reagowanie na zgłoszone incydenty;
- klasyfikowanie incydentów, w tym incydentów poważnych oraz incydentów istotnych, jako incydenty krytyczne oraz
- koordynowanie obsługi incydentów krytycznych;
- przekazywanie do innych państw, w tym państw członkowskich Unii Europejskiej, i przyjmowanie z tych państw informacji o incydentach poważnych i incydentach istotnych dotyczących dwóch lub większej liczby państw członkowskich, a także przekazywanie do Pojedynczego Punktu Kontaktowego zgłoszenia incydentu poważnego i istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej;
- zapewnienie zaplecza analitycznego oraz badawczo-rozwojowego;

- zapewnienie możliwości dokonywania zgłoszeń incydentów oraz udostępnienie i obsługa środków komunikacji pozwalających na dokonywanie tych zgłoszeń;
- tworzenie i udostępnianie narzędzi dobrowolnej współpracy i wymiany informacji o zagrożeniach cyberbezpieczeństwa i incydentach;
- przyjmowanie zgłoszeń dotyczących nielegalnych treści w Internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci.

CSIRT NASK przetwarza dane osobowe wyłącznie na podstawie:

1. obowiązku wynikającego z przepisu prawa, w szczególności ustawy o k.s.c.;
2. uprzedniej dobrowolnej zgody osoby, której dane dotyczą na przetwarzanie jej danych osobowych (np. w przypadku rejestracji na konferencję SECURE lub zgłoszenia incydentu poprzez formularz dostępny na stronie www.incydent.cert.pl);
3. umów zawartych z zaufanymi partnerami i kontrahentami w zakresie informowania o zagrożeniach, podatnościach oraz incydentach;
4. uzasadnionego interesu realizowanego przez CSIRT NASK lub stronę trzecią (np. do celów badań naukowych lub historycznych, a także do celów statystycznych, w związku z ustalaniem, dochodzeniem lub obroną przed roszczeniami).

CSIRT NASK przetwarza dane osobowe wyłącznie w zakresie niezbędnym do realizacji celu, dla którego zostały one zgromadzone.

CSIRT NASK deklaruje funkcjonowanie witryn CSIRT NASK z najwyższą starannością, zasadami wiedzy technicznej oraz zasadami profesjonalizmu zawodowego, jak również zgodności z obowiązującymi przepisami prawa, w szczególności tymi, które chronią prywatność użytkowników witryn internetowych.

W niektórych przypadkach zgłoszenia incydentu z wykorzystaniem formularza na stronie www.incydent.cert.pl, podanie imienia i nazwiska, numeru telefonu oraz adresu poczty elektronicznej osoby zgłaszającej oraz osoby uprawnionej do składania wyjaśnień jest obowiązkowe zgodnie z przepisami ustawy o k.s.c.

W pozostałych przypadkach skorzystanie z formularza zgłaszania incydentu na stronie www.incydent.cert.pl lub www.dyzurnet.pl, osoba, której dane dotyczą ma możliwość podjęcia dobrowolnej decyzji co do udostępnienia lub odmowy udostępnienia swoich danych, niemniej jednak udostępnienie danych osobowych może być wymagane w sytuacji, w której osoba ta zainteresowana będzie otrzymaniem informacji dotyczących obsługi incydentu zgłoszonego w ramach witryny www.incydent.cert.pl.

3. Kategorie danych osobowych

CSIRT NASK przetwarza dane osobowe pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa:

1. dotyczące użytkowników systemów informacyjnych oraz użytkowników telekomunikacyjnych urządzeń końcowych;
2. dotyczące telekomunikacyjnych urządzeń końcowych w rozumieniu art. 2 pkt 43 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne;
3. gromadzone przez operatorów usług kluczowych i dostawców usług cyfrowych w związku ze świadczeniem usług;

4. gromadzone przez podmioty publiczne w związku z realizacją zadań publicznych,
5. dotyczące podmiotów zgłaszających incydent.

4. Okres przechowywania danych osobowych

CSIRT NASK przetwarza dane osobowe przez okres nie dłuższy niż jest to niezbędne dla realizacji celu, w którym dane te są przetwarzane, w szczególności dla obsługi incydentu.

Dane osobowe pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa, niezbędne do realizacji zadań CSIRT NASK, są usuwane lub anonimizowane przez CSIRT NASK w terminie 5 lat od zakończenia obsługi incydentu, którego dotyczą.

5. Udostępnienie danych osobowych

Dane osobowe pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa mogą być przekazywane innym CSIRT-om poziomu krajowego, tj. CSIRT MON i CSIRT GOV, oraz sektorowym zespołom cyberbezpieczeństwa w celu realizacji ich zadań określonych przepisami prawa, w tym w szczególności ustawy o k.s.c.

6. Prawa osób, których dane dotyczą

Przetwarzanie danych osobowych pozyskanych w związku z incydentami i zagrożeniami cyberbezpieczeństwa wymienionych w pkt 3 niniejszej Polityki nie wymaga realizacji obowiązków, o których mowa w art. 15, art. 16, art. 18 ust. 1 lit. a i d oraz art. 19 zdanie drugie Rozporządzenia Parlamentu Europejskiego i Rady UE z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: „RODO”), jeżeli uniemożliwiłoby to realizację zadań CSIRT NASK określonych w ustawie o k.s.c.

W przypadku, gdy warunki określone w zdaniu poprzedzającym nie mają zastosowania, osobie, której dane osobowe przetwarzane przez CSIRT NASK dotyczą, przysługuje prawo żądania: wglądu do swoich danych, ich poprawiania, ograniczenia przetwarzania oraz usunięcia, a ponadto prawo do przeniesienia danych do innego administratora, a jeśli dane przetwarzane są na podstawie zgody - prawo do cofnięcia udzielonej zgody, bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie tej zgody przed jej cofnięciem.

Osobie takiej przysługuje też prawo sprzeciwu wobec przetwarzania jego danych osobowych oraz prawo do wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych.

7. Środki bezpieczeństwa przetwarzania danych osobowych

CSIRT NASK, przetwarzając dane osobowe, prowadzi analizę ryzyka, stosuje środki ochrony przed złośliwym oprogramowaniem oraz mechanizmy kontroli dostępu, a także opracowuje procedury bezpiecznej wymiany informacji.