Klauzula informacyjna (ogólna)

Zgodnie z art. 13 ust. 1 i ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanym dalej RODO), informuję, iż:

1. Administratorem Państwa danych osobowych jest Gminna Spółdzielnia „Samopomoc Chłopska" w Ślesinie reprezentowana przez Prezesa , z siedzibą: ul. Nowomiejska 1, 62-561 Ślesin.
2. Administrator wyznaczył Inspektora Ochrony Danych z którym mogą się Państwo kontaktować za pomocą adresu e-mail inspektor@osdidk.pl.
3. Państwa dane osobowe przetwarzane będą na podstawie:
   - art. 6 ust. 1 lit. c RODO tj. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
   - art. 6 ust. 1 lit. b RODO tj. przetwarzanie jest niezbędne do zawarcia umowy;
   - art. 6 ust. 1 lit. f RODO tj. przetwarzanie jest niezbędne z prawnie uzasadnionych interesów Administratora;
   - art. 6 ust. 1 lit. a RODO tj. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów.
4. Podanie przez Państwo danych osobowych jest obowiązkowe jeżeli podstawę przetwarzania danych stanowi obligatoryjny przepis prawa, w pozostałych wypadkach podanie danych osobowych jest dobrowolne, ale jednocześnie niezbędne i konieczne celem realizacji umowy.
5. Państwa dane osobowe nie będą udostępniane innym odbiorcom z wyłączeniem podmiotów do tego uprawnionych takich jak:
   - podmioty upoważnione do odbioru danych osobowych na podstawie odpowiednich przepisów prawa,
   - podmioty, które przetwarzają dane osobowe w imieniu Administratora na podstawie zawartej z Administratorem umowy powierzenia przetwarzania danych osobowych.
6. Państwa dane osobowe po zrealizowaniu celu, dla którego zostały zebrane, będą przetwarzane w celach archiwalnych i przechowywane przez okres niezbędny wynikający z przepisów dotyczących archiwizacji dokumentów oraz z tytułu przedawnienia ewentualnych roszczeń.
7. W związku z przetwarzaniem Państwa danych osobowych przez Administratora posiadają Państwo prawo do:
   a) dostępu do treści danych na podstawie art. 15 RODO;
   b) sprostowania danych na podstawie art. 16 RODO;
   c) usunięcia danych na podstawie art. 17 RODO jeżeli: dane osobowe przestaną być niezbędne do celów, w których zostały zebrane lub w których były przetwarzane oraz gdy dane są przetwarzane niezgodnie z prawem;
   d) ograniczenia przetwarzania danych na podstawie art. 18 RODO jeżeli osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych.
8. Jeżeli Państwa dane osobowe przetwarzane są na podstawie zgody, posiadają Państwo prawo do wycofania zgody w dowolnym momencie z tym, że wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.
9. Jeżeli uznają Państwo, że przetwarzanie danych narusza przepisy RODO, posiadają Państwo prawo wniesienia skargi do Urzędu Ochrony Danych Osobowych - Prezesa adres ul. Stawki 2, 00-193 Warszawa, e-mail: kancelaria@uodo.gov.pl. tel.: 225310300.
10. Podane przez Państwa dane osobowe nie będą przetwarzane w sposób zautomatyzowany, w tym nie będzie wobec nich profilowania.
11. Państwa dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej.

Kontakt do Inspektora Ochrony Danych Osobowych

Ewa Galińska

tel. Kontaktowy: 531 641 425

e-mail: inspektor@osdidk.pl

CYBERBEZPIECZEŃSTWO

Realizując zadania, wynikające z art. 22 ust. 1 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2023 r. poz. 913, z późn.zm.), przekazujemy Państwu informacje pozwalające na zrozumienie zagrożeń występujących w cyberprzestrzeni oraz porady jak skutecznie stosować sposoby zabezpieczenia się przed tymi zagrożeniami.

Najpopularniejsze zagrożenia w cyberprzestrzeni:

- ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki, itp.),
- kradzieże tożsamości, kradzieże (wyłudzenia), modyfikacje bądź niszczenie danych,
- blokowanie dostępu do usług,
- spam (niechciane lub niepotrzebne wiadomości elektroniczne),
- ataki socjotechniczne (np. phishing, czyli wyłudzanie poufnych informacji przez podszywanie się pod godną zaufania osobę lub instytucję).

Sposoby zabezpieczenia się przed zagrożeniami:

- Zainstaluj i używaj oprogramowania przeciw wirusom i spyware. Najlepiej stosuj ochronę w czasie rzeczywistym.
- Aktualizuj bazy danych wirusów (dowiedz się czy twój program do ochrony przed wirusami posiada taką funkcję i robi to automatycznie).
- Regularnie aktualizuj oprogramowanie na komputerze, szczególnie oprogramowanie przeglądarek internetowych. Hakerzy szukają luk, a producenci cały czas „uszczelniają" wykryte luki w oprogramowaniu. Dzięki aktualizacjom mamy zawsze na komputerze najbardziej odporne na ataki hakerskie oprogramowanie.
- Nie instaluj na komputerze nielegalne oprogramowanie. Może ono zawierać przygotowane przez hakerów wirusy, które pomogą im w opanowaniu naszego komputera, wyłudzeniu danych, i w końcu pozwolą na okradzenie nas.
- Nie otwierajmy wiadomości i dołączonych do nich załączników z nieznanych źródeł. W załącznikach może być ukryte złośliwe oprogramowanie.
- Nie otwieraj plików nieznanego pochodzenia.
- Sprawdzaj pliki pobrane z Internetu za pomocą skanera antywirusowego.
- Nie korzystaj ze stron banków, poczty elektronicznej czy portali społecznościowych, które nie mają ważnego certyfikatu, chyba, że masz stuprocentową pewność z innego źródła, że strona taka jest bezpieczna.
- Dokonuj płatności tylko z własnego komputera lub telefonu. Nie korzystaj do tych celów z publicznej sieci Wi-fi np. na lotnisku, w kawiarence internetowej.
- Pamiętaj, że żaden bank czy Urząd nie wysyła e-maili do swoich klientów/interesantów z prośbą o podanie hasła lub loginu w celu ich weryfikacji.
- Staraj się nie odwiedzać zbyt często stron, które oferują niesamowite atrakcje (darmowe filmiki, muzykę, albo łatwy zarobek przy rozsyłaniu spamu) – często na takich stronach znajdują się ukryte wirusy, trojany i inne zagrożenia.
- Nie zostawiaj danych osobowych w niesprawdzonych serwisach i na stronach, jeżeli nie masz absolutnej pewności, że nie są one widoczne dla osób trzecich.
- Nie wysyłaj w e-mailach żadnych poufnych danych w formie otwartego tekstu.
- Zmieniaj regularnie hasła do swojego komputera oraz dostępu do konta internetowego. Powinny to być hasła trudne i różne do każdej usługi internetowej.
- Pamiętaj o uruchomieniu firewalla.
- Wykonuj kopie zapasowe ważnych danych.

Zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie sposobów zabezpieczania się przed zagrożeniami, to wiedza niezbędna każdemu użytkownikowi komputera, smartphona czy też usług internetowych.

Dodatkowe informacje:

- zestaw porad bezpieczeństwa dla użytkowników komputerów prowadzony na witrynie internetowej CSIRT NASK – Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na poziomie krajowym: https://www.cert.pl/ouch/
- poradniki na witrynie internetowej Ministerstwa Cyfryzacji: https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo
- publikacje z zakresu cyberbezpieczeństwa: https://www.cert.pl/
- strona internetowa kampanii STÓJ. POMYŚL. POŁĄCZ. mającej na celu zwiększanie poziomu świadomości społecznej i promowanie bezpieczeństwa w cyberprzestrzeni: https://stojpomyslpolacz.pl/stp/