FUNDACJA TOGATUS PRO BONO

BIULETYN DLA MŁODZIEŻY

TWOJE PRAWA W ŚWIECIE INTERNETU I MEDIÓW SPOŁECZNOŚCIOWYCH

Zadanie zlecone z zakresu administracji rządowej finansowane ze środków otrzymanych od Powiatu Pruszkowskiego.

Ministerstwo Sprawiedliwości

powiat pruszkowski nieskończone możliwości

Starostwo Powiatowe w Pruszkowie
ul. Drzymały 30
05-800 Pruszków
22 738 14 00

FUNDACJA TOGATUS PRO BONO

Prawa uczniów w świecie Internetu

Ochrona prywatności i bezpieczeństwo w sieci

W dobie Internetu ważną kwestią są prawa uczniów w Internetucie i w mediach społecznościowych w zakresie bezpieczeństwa, prywatności i wolności słowa. W Polsce prawa te reguluje kilka aktów prawnych, m.in. Konstytucja RP, ustawa o prawie autorskim i prawach pokrewnych, ustawa o ochronie danych osobowych (zwana dalej UODO) oraz Konwencja o prawach dziecka. Obowiązują również przepisy unijne tj., rozporządzenie 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 (RODO)

Prawa i wolności jakie przysługują uczniom w Internecie to m.in.:

- prawo do ochrony życia prywatnego i rodzinnego, czci i dobrego imienia (art. 47 Konstytucji),
- wolność porozumiewania się i ochrona tajemnicy komunikowania się (art. 49 Konstytucji),
- wolność sumienia i wyznania religii (art. 53 Konstytucji),
- wolność wyrażania swoich poglądów oraz otrzymywania i rozpowszechniania informacji (art. 54 Konstytucji),
- prawo do zachowania własnej tożsamości, w tym do ochrony osobistej, obywatelstwa, nazwiska czy więzów rodzinnych (art. 8 Konwencji o prawach dziecka),
- ochrona życia prywatnego i rodzinnego (art. 16 Konwencji o prawach dziecka),
- ochrona korespondencji ucznia, w tym tej prowadzonej na portalach społecznościowych (art. 16 Konwencji o prawach dziecka),
- prawo do otrzymywania informacji, w tym również pochodzących ze źródeł zagranicznych (art. 17 Konwencji o prawach dziecka),
- ochrona przed różnymi formami przemocy, w tym nienawiścią czy hejtem (art. 19 Konwencji o prawach dziecka),
- ochrona przed wszelkimi formami wykorzystywania, w tym wykorzystywania seksualnego (art. 34 Konwencji o prawach dziecka),
- prawo do ochrony wizerunku (art. 81 ustawy o prawie autorskim i prawach pokrewnych),
- „prawo do bycia zapomnianym”, czyli prawo do usunięcia z Internetu wszelkich informacji o sobie (art. 17 UODO).

Ochrona danych osobowych i prywatności online

Dane osobowe to informacja, która pozwala na zidentyfikowanie lub stwarza możliwość zidentyfikowania osoby fizycznej. Jako przykład danych osobowych można wymienić: imię i nazwisko, numer PESEL, adres e-mail, numer telefonu, odcisk palca, adres IP, plik cookie, historia przeglądania stron internetowych czy zdjęcie twarzy lub skan oka itp.

Przetwarzanie danych osobowych

Przetwarzanie danych osobowych to każda operacja (czynność), lub ich zbiór, wykonywana na danych osobowych, takich jak: zbieranie, zapisywanie, pobieranie, organizowanie, przechowywanie, modyfikowanie, przeglądanie, wykorzystywanie, ujawnianie, przekazywanie, rozpowszechnianie, łączenie, ograniczanie, usuwanie lub niszczenie. Przetwarzanie danych osobowych może być wykonywane przez podmioty takie jak: administrator danych, podmiot przetwarzający lub odbiorca danych.

Podstawą przetwarzania danych osobowych jest zgoda osoby, której dane dotyczą, poprzez świadome, dobrowolne i jednoznaczne okazanie woli, wyrażone w formie oświadczenia lub wyraźnego działania potwierdzającego. Zgoda ta może być udzielona w różny sposób. Może odbyć się np. poprzez podpisanie formularza zgody, zaznaczenie pola wyboru na stronie internetowej, wysłanie wiadomości e-mail, naciśnięcie przycisku, scan oka itp. Zgoda może być również cofnięta w dowolnym momencie przez osobę, której dane dotyczą.

Ujawnione dane osobowe są przetwarzane przez administratora danych w formie rejestru, dokumentacji kadrowej, księgowej, podatkowej. Niekiedy dane te są zgłaszane do organów administracji publicznej, instytucji prywatnych np. bankowych, wymiaru sprawiedliwości.

Inspektor ochrony danych (IOD), reprezentowany przez dyrektora szkoły, powinien być przygotowany do niezwłocznego podjęcia odpowiednich działań po otrzymaniu informacji o naruszeniu ochrony danych. **Zgodnie z art. 85 RODO brak adekwatnej i szybkiej reakcji może skutkować m.in.: szkodami fizycznymi, szkodami materialnymi lub niematerialnymi wobec osób fizycznych, np.: utratą kontroli nad danymi osobowymi lub ograniczeniem możliwości personalnych, dyskryminacją, kradzieżą lub sfałszowaniem tożsamości, stratą finansową, nieuprawnioną zmianą pseudonimu, zniesławieniem, utratą poufności danych osobowych.** Dyrektor musi również niezwłocznie podjąć działania zgodnie z postanowieniami **art. 33 ust. 1 RODO, zgodnie z którym ma on jedynie 72 godziny na zgłoszenie naruszenia organowi nadzorczemu**. Zgłoszeniu podlegają jedynie te naruszenia, które powodują wysokie ryzyko naruszenia praw i wolności osób fizycznych. W związku z tym dyrektor powinien posiadać wewnętrzne procedury, które pomogą mu ocenić ryzyko, na które narażone są osoby fizyczne, i podjąć decyzję o dokonaniu zgłoszenia. Procedura jest także pomocna w określeniu działań mających na celu ograniczenie skali naruszenia i przywrócenie stanu sprzed naruszenia. Ponadto dyrektor szkoły musi opracować zasady zgłaszania naruszeń podmiotom przetwarzającym informacje. Organ nadzorczy może powiadomić na cztery sposoby:

1. elektronicznie poprzez wypełnienie formularza dostępnego bezpośrednio na stronie danej szkoły,
2. elektronicznie przesyłając wypełniony formularz na skrzynkę elektroniczną ePUAP,
3. elektronicznie wysyłając wypełniony formularz z tekstem ogólnym dostępnym na platformie stronie szkołylub pod adresem epuap.gov. pl,
4. tradycyjną drogą pocztową, przesyłając wypełniony formularz na adres Urzędu Ochrony Danych Osobowych.

Formularz w formie edytowalnego pliku tekstowego dostępny jest na stronie internetowej pod adresem: www.uodo.gov.pl.

Art 33 ust. 3 RODO wskazuje, jakie informacje musi zawierać zgłoszone naruszenie:

1. opis charakteru naruszenia bezpieczeństwa danych osobowych, w miarę możliwości wskazanie kategorii i przybliżonej liczby osób, których dotyczy naruszenie;
2. imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub nazwę innego punktu kontaktowego, w którym można uzyskać dalsze informacje (jeśli został podany);
3. opis możliwych konsekwencji naruszenia danych osobowych;
4. opis środków naprawczych wdrożonych lub planowanych przez administratora w celu usunięcia naruszenia bezpieczeństwa danych osobowych, w tym w razie potrzeby środków mających na celu zminimalizowanie jego ewentualnych negatywnych skutków.

Jeżeli w warunkach zgłoszenia nie jesteśmy w stanie opisać wszystkich negatywnych skutków zdarzenia, należy pamiętać, że bardziej szczegółowe informacje zostaną podane sekwencyjnie w dalszej części. Może się zdarzyć, że początkowo nie będzie potrzeby zgłaszania, ponieważ ryzyko naruszenia praw i wolności osób fizycznych jest niewielkie. Jednak z biegiem czasu sytuacja może się zmienić i należy ponownie przeprowadzić analizę ryzyka i w razie potrzeby sporządzić raport. W takim przypadku można zastosować ogłoszenie publiczne lub inny podobny środek, który równie skutecznie powiadamia dane o naruszeniu bezpieczeństwa danych. Dobrą praktyką jest umieszczanie widocznych banerów lub komunikatów na stronie internetowej szkoły.

Dyrektor ma obowiązek prowadzić wewnętrzny rejestr naruszeń danych osobowych oraz dokumentować wszystkie naruszenia danych osobowych, a także brać pod uwagę okoliczności sprawy oraz kategorie osób i zakres danych osobowych, których dotyczy naruszenie bezpieczeństwa danych, konsekwencje zdarzenia oraz jakie środki naprawcze podjął w związku z negatywnymi konsekwencjami naruszenia, aby zminimalizować konsekwencje. W dokumentach należy także podać uzasadnienie decyzji dyrektora, w przypadku gdy postanowi on nie zgłaszać naruszenia organowi nadzorczemu. We wszystkich zgłaszanych działaniach dyrektora musi wspierać wyznaczony przez niego inspektor ochrony danych. Pamiętaj, że zgodnie z art. 39 RODO jednym z obowiązków inspektora ochrony danych jest pełnienie funkcji osoby kontaktowej dla organu nadzorczego w sprawach związanych z przetwarzaniem.

Niewykonanie obowiązków wynikających z art. 33 i 34, może skutkować karą pieniężną ustaloną przez Prezesa Urzędu Ochrony Danych Osobowych (art. 83 ust. 4 lit.a RODO).

Wolność słowa a granice odpowiedzialności w mediach społecznościowych

Wolność słowa to jedno z podstawowych praw człowieka zagwarantowane przez Konstytucję RP i międzynarodowe konwencje. Oznacza ona możliwość wyrażania swoich poglądów i opinii, a także dostępu do informacji, bez ingerencji władz lub innych podmiotów. Jednak wolność słowa nie jest bezwzględna i nie oznacza, że można mówić lub pisać wszystko, co się chce. Wolność słowa ma swoje granice, które wynikają z prawa i zasad etyki. Nie można naruszać praw i godności innych ludzi, szerzyć nienawiść czy nawoływać do przemocy. Takie zachowania mogą być karane przez sądy lub organy administracyjne.

W Internecie i w mediach społecznościowych wolność słowa jest szczególnie narażona na zagrożenia i nadużycia. Z jednej strony, Internet daje możliwość łatwego i szybkiego komunikowania się z innymi ludźmi, wymiany poglądów i informacji, tworzenia i udostępniania treści. Z drugiej strony, Internet jest przestrzenią, gdzie łatwo dochodzi do naruszeń praw innych osób, takich jak: obraza, zniesławienie, naruszenie prywatności, czy kradzież własności intelektualnej.

Definicja hejtu

Za stosowanie hejtu w Internecie grożą konsekwencje prawne. Aby ustalić o czym mówimy należy zdefiniować pojęcie hejtu. Hejt, to inaczej, obrażanie, ośmieszanie, czy poniżanie innych, a tym samym jest to forma cyberprzemocy. Internecie hejt jest zjawiskiem bardzo częstym. Powodem jest fakt, iż hejter czuje się w Internecie bezkarny. Uważa, że jest postacią anonimową - nikt nie wie, kim naprawdę jest. Nikt jednak nie może (i nie powinien) czuć się bezkarny. W Internecie daje się zauważyć tzw. podwójne standardy, tj. inaczej osoba zachowuje się w tzw. „realu", przy bezpośrednich kontaktach, tzw. „twarzą w twarz", a inaczej w sieci. To zachowanie można częściowo wyjaśnić tak zwanym „efektem pilotażowym". Badanie (Walrave i Heirman, 2009) wykazało, że piloci bombowców bombardowali miasta podczas II wojny światowej bez ponoszenia kosztów emocjonalnych, ponieważ nie widzieli cierpienia swoich ofiar. To samo dotyczy nienawiści w Internecie. Osoba hejtująca nie widzi szkody, jaką wyrządza odbiorcy, dlatego często nie zdaje sobie sprawy, jak bolesne mogą być jej słowa lub zachowanie.

Czym jest hejt?

Prawo do wolności słowa, a więc i możliwość publicznego wyrażania swoich poglądów, gwarantuje nam Konstytucja. Dlatego hejtem nie jest każda wypowiedź krytyczna. O tym, co odróżnia hejt od krytyki, jest sposób wyrażania swego zdania, czy przedstawiania swoich poglądów, tj. merytorycznie, kulturalnie, nie odnosząc się przy tym do kwestii personalnych. Dlatego przed każdym kliknięciem „dodaj komentarz" należy zastanowić się nad tym, czy nasz komentarz:

- obraża daną osobę, gdyż wprost odnosi się do jej cech fizycznych, czy umysłowych, a także czy odnosi się innych elementów związanych z daną osobą i cechami ją opisującymi, np. do jej pochodzenia, wiary, orientacji seksualnej lub ewentualnie zawiera słowa powszechnie uznawane za obraźliwe. Z uwagi na fakt, iż nie ma ścisłej definicji, czym jest tzw. „bezpieczny komentarz", należy zawsze myśleć o tym, co się pisze i w jakiej formie. Tutaj można i należy zastosować regułę: nie czyń drugiemu, co Tobie niemiłe.

Zgłoszenie hejtu

Hejt i cyberprzemoc, to formy agresji i dyskryminacji, naruszające prawa i godność ludzi w sieci. Ich „siła oddziaływania”, czy „rażenia” jest tak potężna, że może skutkować pogorszeniem stanu zdrowia psychicznego i fizycznego ofiar takiej przemocy. Wpływa także negatywnie na atmosferę i jakość życia publicznego.

Jeśli w Internecie mamy materiały szerzące nienawiść, musimy chronić te informacje (zrzut ekranu, nagranie) i przekazać je na Policję w celu zbadania. Jeżeli nienawiść przybierze formę czynu zabronionego z oskarżenia prywatnego, obowiązkiem ofiary jest zebranie dowodów i przygotowanie oskarżenia prywatnego, które zostanie skierowane do sądu. W przypadku nieletnich konieczne jest zgłoszenie materia. nienawiści w szkole, a nawet w ośrodku wsparcia. Obie strony mają możliwość powiadomienia sądu o stwierdzonym zdarzeniu. Bez wątpienia nieletni powinni informować rodziców, jeśli zaobserwują nienawiść skierowaną w stronę innych osób lub sami jej doświadczą. Warto wiedzieć, że mowa nienawiści w Internecie jest monitorowana. Kilka instytucji (fundacji, stowarzyszeń) zajmuje się tym problemem i zachęca do zgłaszania mowy nienawiści, głównie w wybranym przez siebie regionie (np. mniejszości etniczne).Istnieją strony internetowe, portale i grupy, na których można zgłaszać mowę nienawiści np. hejtstop.pl, omzrik.pl, dyzurnet.pl, poznawiecej.org.

NIEODPŁATNE USŁUGI
-POMOC PRAWNA
-PORADY OBYWATELSKIE
-MEDIACJA

NIEODPŁATNA POMOC PRAWNA - NIEODPŁATNE PORADNICTWO OBYWATELSKIE

Na terenie całej Polski funkcjonuje ponad 1500 punktów nieodpłatnej pomocy prawnej i nieodpłatnego poradnictwa obywatelskiego. Jest to rezultat wejścia w życie ustawy o nieodpłatnej pomocy prawnej, nieodpłatnym poradnictwie obywatelskim oraz edukacji prawnej.

Z bezpłatych porad może skorzystać każda osoba, której nie stać na uzyskanie odpłatnej porady i która złoży stosowne oświadczenie.

Prawnicy oraz doradcy **Fundacji Togatus Pro Bono** udzielają bezpłatnych porad prawnych w punktach nieodpłatnej pomocy prawnej na terenie powiatów, z którymi Fundacja zawarła umowy.

Zapraszamy do zapoznania się z zasadami udzielania bezpłatnej pomocy prawnej lub obywatelskiej.

.

Sprawdź, jak i gdzie uzyskać darmową poradę

www.fundacja.togatus.pl

FUNDACJA
TOGATUS
PRO BONO