e-Biuletyn

Powiatu Olsztyńskiego

Nr 3/2020/Ol

Fundacja Rozwoju Ziemi Oleckiej

Publikacja współfinansowana ze środków Powiatu Olsztyńskiego

Szanowni Państwo,

mamy zaszczyt oddać w Państwa ręce e-Biuletyn numer 3/2020 dotyczący wybranych zapytań z Punktu Nieodpłatnego Poradnictwa Obywatelskiego w Stawigudzie w Powiecie Olsztyńskim. W niniejszym numerze przybliżamy różne zagadnienia z zakresu ochrony danych osobowych, z punktu widzenia rodzica dziecka przedszkolnego oraz niepokoje pracownika.

Biuletyn ten powstał w ramach realizacji zadania publicznego przez Fundację Rozwoju Ziemi Oleckiej, współfinansowanego ze środków Powiatu Olsztyńskiego, polegającego na prowadzeniu Punktu Nieodpłatnego Poradnictwa Obywatelskiego w Stawigudzie. W niniejszym wydaniu e-Biuletynu poruszamy najczęstsze problemy, z którymi zgłaszają się Państwo do Punktu NPO.

Do prowadzonego przez nas Punktu Nieodpłatnego Poradnictwa Obywatelskiego w Stawigudzie zapraszamy wszystkie uprawnione osoby w godzinach:

poniedziałek	wtorek	środa	czwartek	piątek
13:00 – 17:00	8:00 – 12:00	8:00 – 12:00	8:00 – 12:00	8:00 – 12:00

Punkt mieści się w Gminnym Ośrodku Pomocy Społecznej w Stawigudzie ul. Olsztyńska 10.

Z wyrazami szacunku,

w imieniu Fundacji Rozwoju Ziemi Oleckiej

Andrzej Wojczulewicz – Prezes Zarządu Fundacji

1. Podpisywanie umowy z przedszkolem – jakich danych nie trzeba podawać

Od września bieżącego roku moje dziecko zostało przyjęte do przedszkola. Kolejnym krokiem było podpisanie umowy o świadczenie usług przedszkolnych. Zainteresowała mnie ilość danych jakie chciała ode mnie uzyskać dyrekcja przedszkola. Czy do przyjęcia mojego dziecka do placówki konieczne jest podanie mojego miejsca zatrudnienia?

Coraz większa liczba rodziców zadaje pytania dotyczące zakresu pozyskiwania danych podczas podpisywania umowy o świadczenie usług przedszkolnych przez podmioty publiczne jak i niepubliczne. Zbierane są dane nie tylko konieczne do zawarcia umowy jak imię i nazwisko rodziców dziecka, adres ich zamieszkania, ale i takich dane jak: numery PESEL rodziców, miejsce zatrudnienia rodziców, informacje o stanie zdrowia dziecka. W tym wypadku zbieranie takich danych stanowi naruszenie nie tylko prawa oświatowego, ale i zasad minimalizacji danych, o których mowa w art. 5 ogólnego rozporządzenia o ochronie danych osobowych.

Do tzw. danych zwykłych należą informacje dotyczące zawodu rodziców i miejsca ich pracy. Przetwarzanie tych danych możliwe jest, gdy spełniona jest jedna z przesłanek określonych w art. 6 ust. 1 ogólnego rozporządzenia o ochronie danych. Nie jest jednak jasne w jakim celu przedszkola przetwarzają dane o życiu zawodowym rodziców dziecka, więc bardzo istotne w tym miejscu jest **spełnienie przez odpowiednią placówkę obowiązku informacyjnego wobec rodziców i uczniów celem wskazania kto jest administratorem danych, na jakiej podstawie prawnej te dane są przetwarzane, w jakim celu i przez jaki okres.**

Przykład: Celem przetwarzania danych na temat miejsca zatrudnienia rodziców dziecka może być konieczność wypełnienia *§ 41 ust. 1 rozporządzenia Ministra Edukacji Narodowej i Sportu z dnia 31 grudnia 2002 r. w sprawie bezpieczeństwa i higieny w publicznych i niepublicznych szkołach i placówkach, o każdym wypadku zawiadamia się niezwłocznie m.in. rodziców (opiekunów) poszkodowanego.* Do wypełnienia wyżej wskazanego obowiązku, przetwarzanie informacji o miejscu pracy rodzica może być niezbędne, w przypadku braku możliwości innej formy kontaktu z rodzicem.

Do tzw. szczególnej kategorii danych należą dane na temat przebytych chorób, hospitalizacji lub stanu psychicznego i emocjonalnego dziecka. Przetwarzanie tych danych jest dozwolone tylko i wyłącznie jeżeli zostanie spełniona jedna z przesłanek wskazanych w art. 9 ust. 2 ogólnego rozporządzenia o ochronie danych osobowych. Niedopuszczalne jest

przetwarzanie danych rodziców i dzieci jeżeli nie wynika to wprost z przepisów prawa. Przedszkole nie może przetwarzać wskazanych danych, ponieważ nie są one warunkiem koniecznym przy rekrutacji dziecka do placówki oraz nie są w żaden sposób związane z obowiązkiem sprawowania opieki nad dzieckiem. **Przetwarzanie tych danych jest możliwe tylko wtedy, gdy rodzice wyrażą na to świadomą, dobrowolną zgodę, którą można wycofać w dowolnym terminie.**

W przedszkolach niepublicznych tak samo jak i publicznych podstawą prawną legalizującą przetwarzanie danych dzieci i ich rodziców lub opiekunów jest wypełnienie obowiązku prawnego ciążącego na administratorze – art. 6 ust. 1 lit. c ogólnego rozporządzenia o ochronie danych osobowych. Przedszkola niepubliczne mogą realizować jeszcze inne obowiązki, bądź w innym zakresie dodatkowe zadania, które nie wynikają wprost z przepisów prawa. W takim przypadku podczas rekrutacji podstawą przetwarzania danych jest prawnie uzasadniony interes administratora – art. 6 ust. 1 lit. f ogólnego rozporządzenia o ochronie danych. Rozporządzenie wskazuje jednak, że interes ten nie może mieć nadrzędnego charakteru wobec podstawowych praw i wolności osoby, w szczególności gdy mówimy o dziecku. W związku z tym przedszkole niepubliczne musi poddać analizie czy dane, które chce przetwarzać nie będą naruszały podstawowych praw i wolności dziecka, jak również jego rodzica czy opiekuna.

Obowiązkiem administratora danych dziecka i rodzica lub jego opiekuna jest spełnienie podczas przetwarzania danych obowiązku informacyjnego (art. 13 ust. 1 i 2 lub art. 14 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych), w którym wskazuje kto jest administratorem danych, jakie dane są przetwarzane, w jakim celu, na jakiej podstawie prawnej tak aby osoba której dane są przetwarzane wiedziała, że odbywa się to zgodnie z prawem.

2. Monitoring poczty elektronicznej pracownika

Jestem pracownikiem jednego z urzędów samorządu terytorialnego. Mój pracodawca podjął decyzję o wprowadzeniu monitoringu poczty elektronicznej pracowników, o czym poinformował nas poprzez wywieszenie ogłoszenia na tablicy ogłoszeń. Czy takie działanie pracodawcy jest zgodne z prawem?

Wprowadzenie przez pracodawcę monitoringu poczty elektronicznej pracownika jest jak najbardziej zgodne z prawem jeżeli pracodawca spełni obowiązki nałożone na niego w tym zakresie.

Pracodawca może wprowadzić monitoring poczty elektronicznej pracownika, gdy jest to niezbędne w jego ocenie do zapewnienia organizacji pracy (m.in. pełne wykorzystanie czasu pracy pracownika oraz narzędzi jakie są mu udostępniane do pracy). Pracodawca jednak musi pamiętać, że taka kontrola pracownika nie może naruszać tajemnicy korespondencji oraz innych dóbr osobistych pracownika.

Obowiązkiem pracodawcy jest poinformowanie pracownika w jakim celu będzie stosował monitoring poczty elektronicznej, powinien również wskazać zakres i sposób zastosowania monitoringu. Wszelkie informacje ustalane są w układzie zbiorowym pracy lub w regulaminie albo w obwieszczeniu.

Poinformowanie pracownika odbywa się zgodnie z art. 22^2 §7 kodeksu pracy. Może mieć to formę pisma skierowanego do pracownika, obwieszczenia na tablicy ogłoszeń, komunikatu skierowanego na e-maila, a nawet informacji skierowanej za pomocą internetu zakładowego.

Istotną informacją jest to, że pracodawca powinien poinformować o wprowadzeniu monitoringu poczty elektronicznej nie później niż **dwa tygodnie przed jego uruchomieniem.**

Podsumowując, jeżeli pracodawca spełnił obowiązki wskazane powyżej, to monitoring został wprowadzony zgodnie z przepisami prawa.

3. Jak chronić swoje dane osobowe?

Kilka tygodni temu hakerzy włamali się na moje konto na portalu społecznościowym tym samym wyłudzając duże sumy pieniędzy od moich znajomych (metodą na blika). Niestety moim błędem było to, że od lat miałam to samo hasło, jak również nie stosowałam żadnych dodatkowych metod weryfikacji czy zabezpieczeń. W jaki sposób mogę ochronić moje dane nie tylko w internecie ale również w życiu codziennym?

Niestety dane osobowe stały się cennym towarem, który jest wykorzystywany w celach marketingowych i sprzedażowych. Zdarzają się sytuacje, kiedy dane użyte są do celów przestępczych przez osoby nieuprawnione do ich posiadania np. tak jak wspomniane wyżej pożyczki czy kredyty.

Każdy z nas może świadomie ograniczyć ryzyko wykorzystania danych nie tylko w celach przestępczych ale również do ochrony swojej prywatności.

Poniżej przedstawiamy kilka zasad jakimi powinniśmy się kierować, aby ochronić nasze dane.

1) Uważaj na to co i komu udostępniasz w Internecie

Często nadmiernie dzielimy się informacjami na swój temat w Internecie, stąd jest on źródłem wiedzy o naszych poglądach, zainteresowaniach czy zachowaniach konsumenckich. Takie dane są szczególnie cenne nie tylko dla działów marketingu różnych firm, ale niekiedy też dla przestępców. Szczególnie takie rzeczy mają miejsce, gdy nasz profil jest w pełni publiczny i może być narażony na użycie naszych danych bez naszej wiedzy i przyzwolenia, oczywiście niezgodnie z celem, dla którego je udostępniliśmy.

2) Nie zostawiaj dokumentów w zastaw

Podczas wypoczynku wypożyczając sprzęt np. kajaki, łódki należy pamiętać aby nie oddawać w zastaw dowodu osobistego, paszportu, prawa jazdy, legitymacji szkolnej lub legitymacji studenckiej. Zgodnie z prawem zatrzymywanie dowodu osobistego bez podstawy prawnej jest karane, natomiast nie wszystkie dane osobowe zawarte we wskazanych wyżej dokumentach są niezbędne dla realizacji celu wypożyczenia sprzętu. Utrata kontroli nad dowodem osobistym naraża na posłużenie się tym dokumentem bez naszej wiedzy i woli, co stwarza niebezpieczeństwo kradzieży tożsamości. Osoby dysponujące kompletem informacji o nas mogą podszyć się pod naszą osobę i np. dokonywać różnych transakcji np. zaciągnięcie kredytu w banku czy wypożyczenie drogiego sprzętu i niezwrócenie go (np. samochodu). Osoby, które

przejmą takiego rodzaju dokument mogą zawrzeć w naszym imieniu różnego rodzaju umowy, np. z zakresu usług telekomunikacyjnych.

3) Nie podawaj danych przez telefon

Unikaj przekazywania danych telefonicznie – szczególnie, gdy to nie Ty inicjujesz rozmowę, ale ktoś dzwoni do Ciebie. Udostępnianie danych na odległość to brak pewności co do tego komu faktycznie dane są przekazane. Upewnij się, komu faktycznie udostępniasz dane w trakcie rozmowy telefonicznej, a jeżeli trzeba zweryfikuj kontakt, np. oddzwaniając i sprawdzając, czy dany numer i osoba faktycznie reprezentuje podmiot, na który się powołała.

4) Nie wyrzucaj danych na śmietnik, dopóki nie zostaną zniszczone

Wszelkie dokumenty z naszymi danymi to kolejne źródło wiedzy o nas, zwłaszcza gdy zawierają one wiele różnych informacji np. gdzie pracujemy ile zarabiamy, ile mamy dzieci, jak drogie robimy zakupy. Dlatego też zanim wyrzucisz dokumenty do kosza, należy je zniszczyć (np. faktury, rachunki), zapiski, naklejki na opakowaniach od korespondencji czy po dostarczonych towarach, w sposób uniemożliwiający odtworzenie zawartych w nich danych osobowych.

5) Usuwaj trwale dane z nośników

Wiele danych o nas znajduje się na starych dyskach twardych, kartach pamięci, pendrive'ach czy innych nośnikach. Coraz więcej informacji na nasz temat jest zapisanych w komputerach, smartfonach, aparatach fotograficznych czy tabletach. Zanim pozbędziemy się takich urządzeń lub nośników należy trwale usunąć z nich dane. Jednak zwykłe ich skasowanie nie będzie wystarczające, gdyż wiele danych da się odzyskać. Dlatego zanim wyrzucimy nośnik albo go sprzedamy powinniśmy usunąć z niego dane korzystając przy tym z odpowiedniego do tego oprogramowania. Warto też przywrócić ustawienia fabryczne urządzenia, aby nie było w nim zapamiętanych loginów i haseł do różnych usług i aplikacji z jakich korzystaliśmy, a zwłaszcza z takich, z których nadal korzystamy.

6) Używaj programów chroniących komputer

Ważne jest aby używać oprogramowania chroniącego komputer i urządzenia mobilne przed niepożądanymi działaniami z zewnątrz np. złośliwego oprogramowania. Oprócz popularnych programów antywirusowych przydatne mogą być również te, które zabezpieczą przed ingerencją z zewnątrz tzw. firewall.

7) Bądź czujny w sieci

W sieci:

- nie należy odpowiadać na e-maile od osób, których nie znasz, zwłaszcza gdy domagają się podania informacji o nas, czy namawiają do kliknięcia w przesłany link lub otwarcia przesłanego załącznika.
- należy zachować ostrożność przy korzystaniu z usług bankowości elektronicznej i dokonywaniu zakupów przez Internet, w szczególności zwracać uwagę czy aby na pewno logujemy się do serwisu bankowości internetowej ze strony banku, która ma certyfikat SSL (widoczny w pasku adresu przeglądarki). Sklepy w których chcemy coś kupić powinniśmy dobrze weryfikować: czy w ogóle istnieją, czy i jakie mają opinie, czy są to podmioty zidentyfikowane, gdzie mają siedzibę, czy podany jest kontakt z ich właścicielem i czy kontakt ten nie jest ograniczony tylko do elektronicznego.

8) Zmieniaj hasła

Jedną z najważniejszych zasad ochrony swoich danych jest regularne zmienianie hasła dostępu do swojego komputera, do poczty elektronicznej, systemów bankowości elektronicznej ale nawet sklepów internetowych, w których mamy konto użytkownika. Oczywiście hasła powinny być różne, nigdy nie powinny się powtarzać. Dobrze jest aby nie miały one nic wspólnego z życiem osobistym, miejscem zamieszkania, imieniem i nazwiskiem, datą urodzin itp., aby nie były łatwe do odgadnięcia.

Przestrzeganie tych kilku prostych zasad pomoże nam bezpiecznie zarządzać naszymi danymi i ochroni nas przed ich bezprawnym wykorzystaniem w celach przestępczych, jak również ochroni naszą prywatność.

4. Zasady stosowania monitoringu wizyjnego w miejscu pracy

W firmie, w której jestem zatrudniona zauważyłam, że zamontowane zostały kamery nie tylko na korytarzach ale również w szatni, w której pracownicy przebierają się przed i po zakończeniu pracy. Szef nie poinformował nas, że zamierza wprowadzić monitoring. Czy takie działanie pracodawcy jest zgodne z prawem?

Takie działanie pracodawcy oczywiście nie jest zgodne z prawem. Zasady stosowania monitoringu wizyjnego w miejscu pracy reguluje Kodeks pracy, ale również ogólne rozporządzenie o ochronie danych osobowych, ponieważ w momencie nagrywania obrazu przez kamery, obejmującego wizerunek pracowników, dochodzi do przetwarzania danych osobowych.

Pracodawca kiedy decyduje się na założenie monitoringu w miejscu pracy powinien określić konkretny cel, w którym będzie on wykorzystywany. Monitoring ma służyć zapewnieniu bezpieczeństwa pracowników, ochrony mienia, kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, a obszar nadzoru może obejmować teren zakładu pracy lub teren wokół zakładu pracy.

Pracodawca powinien poinformować osoby, które mogą zostać objęte monitoringiem, o tym, że monitoring jest stosowany i jaki obszar jest nim objęty. Powinien spełnić obowiązek informacyjny wynikający z art. 13 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych czyli m.in. podać nazwę administratora danych, adres, obszar oraz cel monitorowania, okres przetwarzania danych, ewentualnych odbiorów tych danych i co najważniejsze poinformować pracownika o jego prawach.

Pracownicy muszą mieć świadomość, że w miejscu pracy wprowadzono monitoring. **Pracodawca zgodnie z kodeksem pracy oznacza pomieszczenia i teren monitorowany w sposób widoczny i czytelny, za pomocą odpowiednich tablic i klauzul informacyjnych, nie później niż jeden dzień przed jego uruchomieniem.**

Monitoring zastosowany przez pracodawcę **nie może nagrywać dźwięku**. Stosowanie kamer rejestrujących również dźwięk może zostać uznane za naruszenie prywatności oraz za nadmiarową formę przetwarzania danych (chyba że odpowiednie przepisy prawa to regulują). Nieuregulowane prawem rejestrowanie dźwięku może wiązać się z odpowiedzialnością pracodawcy nie tylko administracyjną, cywilną ale i karną. Jak również w trakcie nagrania obrazu i dźwięku za pośrednictwem kamery będzie dochodzić do ujawnienia tajemnic chronionych prawem.

Bardzo ważne jest również to, że kodeks pracy zawiera zamknięty katalog miejsc, w których założenie monitoringu **jest zabronione.** Są to np. łazienki, szatnie czy pomieszczenia socjalne, chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne do realizacji określonego celu i nie naruszy to godności oraz innych dóbr osobistych pracownika. Monitoring pomieszczeń sanitarnych wymaga uzyskania uprzedniej zgody np. związków zawodowych lub przedstawicieli pracowników, albo samych pracowników. Obszar monitorowany powinien zostać również ograniczony do niezbędnego zasięgu, tak aby przetwarzać dane, które są niezbędne do realizacji celu, w jakim monitoring został zastosowany. Pracodawca nie może wykraczać poza katalog zamknięty kodeksu pracy i stosować monitoring w tak szczególnych miejscach do oceny jakości wykonywanej pracy przez pracowników. Takie działanie pracodawcy narusza prywatność pracowników.

W związku z powyższym w opisanej sytuacji pracodawca złamał przepisy nie tylko kodeksu pracy ale również ogólnego rozporządzenia o ochronie danych osobowych. Pracodawca nie poinformował o zastosowaniu monitoringu jak również naruszył prywatność pracowników poprzez umieszczenie kamer w szatniach nie mając do tego odpowiedniego celu i zgody pracowników lub ich przedstawiciela.

Biuletyn opracował:

Specjalista ds. ochrony danych osobowych Malwina Bruździak

Fundacja Rozwoju Ziemi Oleckiej

19- 400 OLECKO ul. Wojska Polskiego 13
tel. 87 520 21 59
e-mail: biuro@fundacja.olecko.pl strona www: www.fundacja.olecko.pl