**NAJWAŻNIEJSZE REGUŁY PRZETWARZANIA DANYCH OSOBOWYCH**

**W PRZEDSZKOLU NR 13 WE WROCŁAWIU**

Poniżej znajdziesz najważniejsze informacje wytyczne w obszarze ochrony danych osobowych. Wydrukuj ten dokument, umieść przy swoim stanowisku pracy i stosuj się do tych kilku prostych, ale bardzo ważnych zasad.

**Na początek bardzo ważna informacja – obalenie mitu o zgodzie**

Potocznie uznaje się, że zgoda osoby fizycznej jest wyłączną przesłanką przetwarzania jej danych osobowych. **Nie jest to prawda**. Jest to jednocześnie jeden z najczęstszych błędów z jakimi się spotkasz w rozmowach z rodzicami, petentami, współpracującymi firmami i wykonawcami.

Prawo przewiduje pięć różnych podstaw przetwarzania danych osobowych dla organów publicznych i w codziennej praktyce zgoda jest drugą od końca **najrzadziej** wykorzystywaną podstawą przetwarzania.

Te najczęściej występujące w Twoim Przedszkolu podstawy przetwarzania to:

1. Wykonywanie obowiązku wynikającego z przepisu prawa
2. Wykonywanie władzy publicznej lub działanie w interesie publicznym
3. Zawarcie umowy

Przykładowo Twoje Przedszkole nie musi w ogóle uzyskiwać odrębnej zgody z obszaru ochrony danych osobowych w sytuacji, gdy:

* zawierana jest umowa o pracę z pracownikiem
* rodzic składa wniosek o rekrutację dziecka do Przedszkola
* dziecko bierze udział w konkursie przedszkolnym
* zawierana jest umowa z kontrahentem

i wiele innych.

I nie chodzi tu o to, że przystąpienie do umowy, czy też złożenie wniosku o rekrutację jest domniemaną zgodą. Nie. Tutaj po prostu w ogóle zgoda nie jest potrzebna. Jeżeli rodzic złoży wniosek o rekrutację do Przedszkola to Przedszkole ma prawny obowiązek rozpatrzyć tę aplikację i zgoda lub jej brak nie ma tu nic do rzeczy. Z kolei jeżeli Przedszkole podpisało umowę o pracę z pracownikiem, to pracownik ten nie może np. nagle cofnąć zgody na przetwarzanie jego danych osobowych i żądać, ażeby Przedszkole go „zapomniało”. Przedszkole ma obowiązek prowadzić dokumentację prawa pracy, rozliczyć podatki, ZUS, szkolenia BHP i inne.

Zgoda na przetwarzanie danych osobowych w Przedszkolu będzie występowała wyjątkowo. Znajdzie ona zastosowanie w sytuacji, w której placówka będzie chciała wykorzystywać zdjęcia zawierające wizerunek dzieci w Internecie, w tym na swojej stronie www. Takie publiczne wykorzystanie wizerunku, pomimo że znajduje się w granicach interesu publicznego realizowanego przez Przedszkole, to jednak w sposób na tyle istotny wpływa na prawa i wolności osób, których dane dotyczą, że wymagana jest ich odrębna zgoda na takie działanie.

O ile wykorzystywanie takiego wizerunku na potrzeby tablo, gabloty na korytarzu, gazetki przedszkolnej (w wersji drukowanej) mieści się w granicach przygotowania dziecka do życia w społeczeństwie, o tyle publikowanie wizerunku dziecka w Internecie jest już czymś ponad, i brak jest innej możliwej podstawy przetwarzania niż zgoda.

Co więc dla przypadków, gdy Przedszkole może przetwarzać dane i nie musi pod to zbierać żadnej zgody? Generalnie nic – Przedszkole może po prostu przetwarzać te dane i zobowiązane jest przy tym zapewnić ich poufność, o czym mowa w dalszej części niniejszego dokumentu.

Jednocześnie, jeżeli dane o określonej osobie / dziecku zebraliśmy po raz pierwszy w historii Przedszkola to konieczne jest przekazanie osobie, której dane dotyczą klauzuli informującej o zasadach przetwarzania danych osobowych. Klauzulę taką wręczamy jednak tylko raz – przy okazji pierwszego kontaktu.

**Jak zachować bezpieczeństwo danych osobowych**

Pamiętaj, że Twoim najważniejszym codziennym obowiązkiem jest zapewnienie poufności danych osobowych. Odpowiedni poziom poufności zapewnisz już stosując się do poniższych 12 prostych zasad.

1. Na koniec dnia uprzątnij biurko. Włóż wszystkie dokumenty nad którymi aktualnie pracujesz do szuflady biurka / do szafki i zamknij je na klucz. Pod Twoją nieobecność w pokoju mogą przebywać inne osoby (np. osoby sprzątające), które nie powinny mieć dostępu do informacji zawartych na dokumentach.
2. Jeżeli zabierasz ze sobą do domu lub w podróż służbowe urządzenia i/lub dokumenty papierowe, miej je generalnie przy sobie do czasu umieszczenia w bezpiecznym i zamkniętym pomieszczeniu (np. mieszkanie, dom, pokój hotelowy). W szczególności nie zostawiaj niczego na noc w samochodzie. Nie zostawiaj niczego bez opieki w przedziale pociągu lub w luku bagażowym samolotu.
3. Nie oddawaj osobie, która nie ma upoważnienia do przetwarzania tych samych danych co Ty, kluczy do Twojego pokoju, do Twoich szafek i biurka, w których przechowujesz dokumenty.
4. Nie podawaj nikomu swojego hasła do komputera lub do systemów bazodanowych.
5. Ustalaj bezpieczne i niepowtarzalne hasła do komputera i systemów informatycznych. Jeżeli gdzieś je zapisujesz nie rób tego na kartce obok stanowiska pracy. Zapisz je na przykład w swoim telefonie komórkowym, do którego dostęp zabezpieczony jest kodem PIN.
6. Stosuj hasło lub PIN w swoim telefonie komórkowym.
7. Nie loguj się do systemów informatycznym jednostki z urządzeń nie firmowych (np. komputer domowy, telefon prywatny albo urządzenia innych osób). Nie są zabezpieczone przez informatyków jednostki i mogą mieć różne szkodliwe oprogramowania.
8. Jeżeli wysyłasz e-mailem dane osobowe poza jednostkę upewnij się, czy odbiorca stosuje protokół szyfrowania korespondencji e-mail. Jeżeli tego nie wiesz, konieczne umieść dane osobowe w pliku i zabezpiecz dostęp do pliku hasłem. Hasło do pliku prześlij do odbiorcy innym środkiem komunikacji niż e-mail.
9. Przesyłając wiadomość e-mail do wielu adresatów, którzy nie znają się nawzajem (np. korespondencja zbiorcza) zamieść ich adresy w ukrytej kopii. W ten sposób nie dojdzie do nieautoryzowanego ujawnienia adresów e-mail osobom nieuprawnionym.
10. Nie wykonuj zadań służbowych, w ramach których przetwarzane są dane osobowe, z wykorzystaniem prywatnej skrzynki e-mail (w tym korespondencja z rodzicami, przesyłanie informacji o uczniach, baz danych).
11. Nie otwieraj załączników przesłanych przez niezaufanego nadawcę, co do którego masz jakiekolwiek wątpliwości (informacje z nieznanego źródła, albo z nieznanych adresów e-mail dot. wystawionych faktur, zaległych lub należnych płatności). Zweryfikuj dokładnie adres e-mail, z którego nadano korespondencję, spróbuj zorientować się czego może dotyczyć temat. Jeżeli cały czas masz wątpliwości zadzwoń pod wskazany w stopce numer telefonu i dopytaj się czego dotyczy temat. Jeżeli wątpliwości nie da się rozstrzygnąć, nie otwieraj załącznika do wiadomości e-mail.
12. Zamieszczając pliki z danymi osobowymi na dysku sieciowym – upewnij się, że jest to dysk, do którego dostęp mają tylko osoby uprawnione do przetwarzania tych danych.

Chociaż powyższe zasady nie są trudne do realizacji, to jednocześnie ich częste łamanie odpowiada za 60% wszystkich naruszeń w obszarze ochrony danych osobowych. Wynika to z faktu, że ludzie z czasem często świadomie zaprzestają stosowania zasad bezpieczeństwa, ponieważ nie należą one do wygodnych. Twoim zadaniem jest wytrwać przy stosowaniu powyższych zasad i nie być źródłem incydentu w obszarze ochrony danych osobowych.

**Praktyczne rady jak działać na co dzień w obszarze ochrony danych osobowych**

1. Jeżeli jakaś osoba (rodzic, podopieczny, kontrahent, były pracownik lub inna osoba) bezpośrednio do Ciebie napisze z żądaniem, powołując się na przepisy o ochronie danych osobowych, w tym na „prawo do bycia zapomnianym”, „prawo do przenoszenia danych”, „prawo dostępu do treści przetwarzanych danych” – nie odpowiadaj samodzielnie. To może być próba wyłudzenia danych lub działanie nakierowane na wprowadzenie w błąd. Przekieruj taką wiadomość do przełożonego lub wyznaczonego w organizacji Inspektora Ochrony Danych (inspektor@coreconsulting.pl).
2. Jeżeli w Twoim otoczeniu dojdzie do jakiegoś incydentu z obszaru przetwarzania danych – np. bezpowrotna utrata danych, zgubienie nośnika danych, wyciek danych – niezwłocznie poinformuj o tym przełożonego lub wyznaczonego w organizacji Inspektora Ochrony Danych (inspektor@coreconsulting.pl). W istotnych przypadkach organizacja ma tylko 72h na przeprowadzenie postępowania wyjaśniającego i powiadomienie Prezesa Urzędu Ochrony Danych Osobowych. I **nie są to** 72h robocze.
3. Jeżeli jakiś zewnętrzny podmiot prosi Cię o podanie danych ucznia, rodzica, przedstawiciela – upewnij się, że na pewno możesz podać te dane. Sprawdź:
	1. kto dokładnie prosi Cię o podanie danych – jaka organizacja, zweryfikuj adres e-mail
	2. w jakim celu masz podać te dane – czy na pewno ten cel jest właściwy, zgodny z prawem
	3. jeżeli o podanie danych prosi Cię podwykonawca jednostki – zweryfikuj czy na pewno jednostka ma z nim podpisane właściwe umowy dot. przekazywania takich danych
	4. czy organ państwa ma podstawę żądać takich informacji (jeżeli masz wątpliwości, skontaktuj się z inspektorem ochrony danych osobowych).

Jeżeli cały czas masz wątpliwości czy możesz podać określone dane skontaktuj się z wyznaczonym w Przedszkolu Inspektorem Ochrony Danych (inspektor@coreconsulting.pl).