Regulamin Ochrony
Danych Osobowych

Administrator

Agata Ciołek

prowadząca działalność gospodarczą pod firmą

EcoChic Organic Beauty Studio

SPIS TREŚCI

1 Wstęp ... 3
2 Zabezpieczenie dokumentacji papierowej z danymi osobowymi ... 3
3 Zasady wynoszenia danych poza firmę/organizację ... 3
4 Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych ... 3
5 Obowiązek zachowania poufności i ochrony danych osobowych ... 4
6 Postępowanie dyscyplinarne ... 4

1 WSTĘP

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO dla:

- Pracowników posiadających dostęp do danych osobowych przetwarzanych przez Administratora;
- Współpracowników posiadających dostęp do danych osobowych przetwarzanych przez Administratora;

2 ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

1. Pracownicy są zobowiązani do stosowania Polityki czystego biurka. Polega ona na zabezpieczaniu (zamykaniu na klucz) dokumentów oraz nośników np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób postronnych.
2. Pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach.
3. Zabrania się pozostawiania dokumentów w miejscach dostępnych dla osób postronnych.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik.

3 ZASADY WYNOSZENIA DANYCH POZA FIRMĘ/ORGANIZACJĘ

1. Pracownicy nie mogą wynosić na zewnątrz dokumentacji zawierającej dane osobowe bez zgody Administratora.
2. W przypadku konieczności przewożenia dokumentacji należy zapewnić bezpieczne jej przewożenie w plecakach, teczkach w celu zabezpieczenia ich przed zagubieniem i kradzieżą.
3. Pracownicy nie mogą wynosić na zewnątrz bez zgody Administratora nośników z danymi osobowymi (np. przenośnych dysków twardych, pen-drive, płyt CD, DVD, pamięci typu Flash zawierających skany lub zdjęcia dokumentacji papierowej gromadzonej przez Administratora).
4. Elektroniczne wersje danych osobowych (np. skany lub zdjęcia dokumentacji papierowej gromadzonej przez Administratora) wynoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski przenośne, zahasłowane pliki, zabezpieczone smartfony).

4 SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Administratora w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Do sytuacji wymagających powiadomienia, należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
    b. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka, niezamykanie pomieszczeń, szaf, biurek)
3. Do incydentów wymagających powiadomienia, należą:

a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania,);
b. zdarzenia losowe wewnętrzne (pomyłki pracowników, utrata / zagubienie danych);
c. umyślne incydenty (włamanie do pomieszczeń, kradzież danych, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych).

4. Typowe przykłady incydentów wymagające reakcji:
   a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
   b. dokumentacja jest niszczona bez użycia niszczarki;
   c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
   d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe;
   e. wynoszenie danych osobowych w wersji papierowej na zewnątrz organizacji bez upoważnienia Pracodawcy;
   f. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;
   g. telefoniczne próby wyłudzenia danych osobowych;

5 OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

1. Każda z osób dopuszczonych do przetwarzania danych osobowych jest zobowiązana do:
   a. przetwarzania danych osobowych wyłącznie w celu i zakresie powierzonych jej zadań,
   b. zachowania w tajemnicy danych osobowych do których ma dostęp,
   c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych jej zadań,
   d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych.
2. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować.
3. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się podstawą prawną do dostępu do takich danych.
4. Każda z osób dopuszczonych do przetwarzania danych osobowych jest zobowiązana do zabezpieczenia danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

6 POSTĘPOWANIE DYSCYPLINARNE

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Administratora za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.