Polityka Ochrony Danych Osobowych w firmach

Bosky sp. z o.o.

Bosky.pl Sp. z o.o. sp.k.

1 Wstęp 3
2 Analiza ryzyka 3
3 Upoważnienia 3
4 Środki techniczne i organizacyjne zabezpieczające dane osobowe 3
5 Regulamin Ochrony Danych Osobowych 4
6 Dodatkowe informacje dotyczące strony www 4
7 Instrukcja postępowania z incydentami 5
8 Kontakt do Administratora DO 5

1 WSTĘP

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Zgodnie z art. 26 powyższego Rozporządzenia firmy Bosky sp. z o.o i Bosky.pl Sp. z o.o. sp.k na mocy zawartych umów są Współadministratorami Danych Osobowych w rozumieniu RODO

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

2 ANALIZA RYZYKA

Procedura zawarta w załączniku 02d_Analiza ryzyka opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

3 UPOWAŻNIENIA

1. Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach (dla kategorii osób) w postaci papierowej oraz w systemach informatycznych
2. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa
3. Upoważnienia nadawane są do zbiorów na wniosek przełożonych osób. Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie – patrz załącznik 01d Upoważnienie do przetwarzania danych osobowych
4. Administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Ewidencja ma charakter pomocniczy i nie jest wymagana przepisami RODO. Patrz załącznik 01c Ewidencja osób upoważnionych
5. W przypadku powierzenia przetwarzania danych do Podmiotu przetwarzającego, Administrator jest zobowiązany do sporządzenia z nim umowy powierzenia, stanowiącą podstawę upoważnienia dla osób z Podmiotu przetwarzającego - patrz załącznik 01f Umowa powierzenia uniwersalna

4 ŚRODKI TECHNICZNE I ORGANIZACYJNE ZABEZPIECZAJĄCE DANE OSOBOWE

1. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych, patrz załącznik Instrukcja zarządzania RODO
2. W instrukcji wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne i organizacyjne
3. Instrukcja jest aktualizowana, jeśli zajdzie taka potrzeba po przeprowadzeniu analizy ryzyka

5 REGULAMIN OCHRONY DANYCH OSOBOWYCH

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania. Patrz załącznik - 04 Regulamin Ochrony Danych Osobowych

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania poprzez podpisanie oświadczenia o poufności zawartego w arkuszu 01c Ewidencja osób upoważnionych

6 DODATKOWE INFORMACJE DOTYCZĄCE STRONY WWW

Poniżej zebrano informacje dotyczące obowiązywania Polityki ODO w zakresie strony www, niezależnie od występowania tych informacji w innych częściach dokumentu

1. Adres naszej witryny internetowej: www.bosky.pl.
2. Dobrowolne podanie danych w formularzu kontaktowym (imię nazwisko, adres email, nr telefonu) jest traktowane jako wyrażenie zgody na ich przetwarzanie.
3. Ciasteczka (Cookies):
    a. Strona tworzy pliki „cookies” (tzw. ciasteczka) stanowiące dane informatyczne, w szczególności pliki tekstowe, które przechowywane są w urządzeniu końcowym Użytkownika strony WWW.
    b. Są one używane w celu optymalizacji procesu korzystania ze stron WWW. Stosowane są również w celu gromadzenia danych statystycznych, które pozwalają identyfikować sposób korzystania użytkowników ze stron internetowych. Daje to możliwość późniejszego ulepszania struktury i zawartości strony WWW.
    c. Pliki „cookies” są usuwane najpóźniej po roku od utworzenia na podstawie daty ich ważności, przy czym usunięcie (czyszczenie) plików cookies zależy od ustawień przeglądarki, będących w gestii Użytkownika.
4. Osadzone treści z innych witryn:
    a. Artykuły na tej witrynie mogą zawierać osadzone treści (np. filmy, obrazki, artykuły itp.). Osadzone treści z innych witryn zachowują się analogicznie do tego, jakby użytkownik odwiedził bezpośrednio konkretną witrynę.
    b. Witryny mogą zbierać informacje o tobie, używać ciasteczek, dołączać dodatkowe, zewnętrzne systemy śledzenia i monitorować twoje interakcje z osadzonym materiałem, włączając w to śledzenie twoich interakcji z osadzonym materiałem jeśli posiadasz konto i jesteś zalogowany w tamtej witrynie.
5. Z kim dzielimy się danymi:
    a. Dane dotyczące przeglądania strony i wpisane do formularza kontaktowego mogą być widoczne dla firm związanych z technicznym zapewnieniem działania strony: hostującej stronę, zarządzającej zawartością strony, zarządzającej serwerem pocztowym, itp..
    b. Ponadto dane są automatycznie przetwarzane przez zewnętrznych usługodawców weryfikujących czy dane w formularzu nie są spamem, nie zostały wypełnione przez bota., lub w celu analizy ruchu na stronie.
6. Dane podane w formularzu kontaktowym przechowujemy bezterminowo (lub do momentu wycofania zgody na ich przetwarzanie z zastrzeżeniem p.7)
7. Użytkownik strony ma prawo do żądania usunięcia lub modyfikacji danych podanych w formularzu. Żądanie usunięcia zostanie spełnione o ile nie zachodzą przesłanki prawne lub dotyczące bezpieczeństwa obligujące Administratora do ich zachowania. W każdym przypadku żądanie usunięcia oznacza wycofanie zgody na przetwarzanie DO w celach marketingowych.

7 INSTRUKCJA POSTĘPOWANIA Z INCYDENTAMI

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

8. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego (lub – Inspektora Ochrony Danych)
9. Do typowych podatności bezpieczeństwa danych osobowych należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)
10. Do typowych incydentów bezpieczeństwa danych osobowych należą:
    a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
    b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
    c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)
11. W przypadku stwierdzenia wystąpienia incydentu, Administrator (lub IOD) prowadzi postępowanie wyjaśniające w toku, którego:
    a. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki
    b. inicjuje ewentualne działania dyscyplinarne
    c. działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu
    d. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia
12. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze – patrz załącznik 03 Formularz rejestracji incydentu
13. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych
14. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

8 KONTAKT DO ADMINISTRATORA DO

Wszelkie sprawy z zakresu Ochrony Danych Osobowych, w tym pytania dotyczące niniejszego dokumentu lub jego załączników, należy kierować na adres email: IOD@bosky.pl