POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

w

W&H Sp. z. o.o.

ul. Kościuszki 49, 44-351 Turza Śląska, NIP: 647-236-13-00

ROZDZIAŁ I

Postanowienia ogólne

§ 1

- Kierownictwo **W&H Sp. z. o.o. ul. Kościuszki 49 44-351 Turza Śląska** świadome wagi problemów związanych z przetwarzaniem i ochroną danych osobowych przyjmuje niniejszy dokument i deklaruje nadzór nad jego przestrzeganiem, aby zapewnić poszanowanie prawa do prywatności, poprzez zastosowanie koniecznych i celowych środków do zabezpieczenia prawidłowego zarządzania przepływem chronionych prawem informacji, dotyczących osób fizycznych, w **W&H Sp. z. o.o. ul. Kościuszki 49 44-351 Turza Śląska**
- Kierownictwo deklaruje zapewnić ochronę danych osobowych na poziome, który odpowiada charakterowi przetwarzanych informacji i pozwala zabezpieczyć je przed bezprawnymi działaniami (bezpieczeństwo informacji).
- Celem polityki bezpieczeństwa ochrony danych osobowych jest dostosowanie technicznych i organizacyjnych środków ochrony w **W&H Sp. z. o.o. ul. Kościuszki 49 44-351 Turza Śląska** do najwyższych standardów ochrony informacji, co umożliwi prawidłowe współużytkowanie wewnątrz organizacji.
- Zarządzanie przetwarzaniem i ochroną danych osobowych **W&H Sp. z. o.o. ul. Kościuszki 49 44-351 Turza Śląska** stanowi uporządkowany i ciągły proces, którego składnikami są: identyfikacja i szacowanie ryzyka, ustanawianie i ulepszanie zabezpieczeń, podnoszenie kwalifikacji personelu oraz wdrożenie procedury i zasad odpowiedzialności za wypadki naruszenia Polityki.

§ 2

Niniejszy dokument jest zbiorem reguł i praktycznych wskazówek określających sposoby prawidłowego zarządzania, ochrony i dystrybucji danych osobowych, w szczególności:

- zasady bezpieczeństwa stosowane podczas przetwarzania danych osobowych;
- organizacyjne i techniczne środki zabezpieczenia danych osobowych przed bezprawnym przetwarzaniem;
- zasady przekazywania danych osobowych między użytkownikami i innymi osobami uprawnionymi;
- warunki odpowiedzialności osób naruszających Politykę;
- zasady zgłaszania administratorowi danych przypadków nieprawidłowości w przetwarzaniu lub ochronie danych osobowych;
- obowiązki użytkowników w zakresie podnoszenia kwalifikacji w dziedzinie ochrony danych osobowych;
- inne informacje, o których mowa w § 4 rozporządzenia ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
- Ustanowione w niniejszym dokumencie zasady odnoszą się do ochrony danych osobowych przetwarzanych zarówno w systemach informatycznych jak i poza nimi.

§ 3

Obowiązek przestrzegania zasad opisanych w niniejszym dokumencie ciąży na:

- wszystkich osobach zatrudnionych w **W&H Sp. z. o.o. ul. Kościuszki 49 44-351 Turza Śląska** również na podstawie umowy cywilno-prawnej;
- stażystach, wolontariuszach, praktykantach i innych osobach działających na rzecz **W&H Sp. z. o.o. ul. Kościuszki 49 44-351 Turza Śląska** w podobnym charakterze;
- członkach organów **W&H Sp. z. o.o. ul. Kościuszki 49 44-351 Turza Śląska**
- innych osobach, które uczestniczą w przetwarzaniu danych osobowych w **W&H Sp. z. o.o. ul. Kościuszki 49 44-351 Turza Śląska**

§ 4

Ilekroć w niniejszym dokumencie jest mowa o:

- ustawie - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
- Polityce – rozumie się przez to niniejszy dokument;
- Instrukcji – rozumie się przez to „Instrukcję Zarządzania Systemem Informatycznym” wydaną przez administratora danych;
- zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
- przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
- systemie informatycznym - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
- administratorze danych - rozumie się przez to **W&H Sp. z. o.o. ul. Kościuszki 49 44-351 Turza Śląska** administratorze bezpieczeństwa informacji – rozumie się przez to osobę powołaną przez administratora danych do pełnienia funkcji administratora bezpieczeństwa informacji na zasadach określonych w ustawie;
- użytkowniku – rozumie się przez to osobę upoważnioną przez administratora danych do przetwarzania danych osobowych;
- identyfikatorze użytkownika - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- haśle - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- rozliczalności - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
- integralności danych - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
- poufności danych - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
- uwierzytelnianiu - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

- Pojęciom niezdefiniowanym w Polityce nadaje się takie znaczenie jakie mają one na gruncie ustawy i wydanych na jej podstawie aktów wykonawczych.

§ 5

W&H Sp. z. o.o. ul. Kościuszki 49 44-351 Turza Śląska przetwarza i zbiera dane osobowe wyłącznie w wypadkach i dla celów dopuszczalnych przez ustawę, w szczególności jeśli:

- osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych;
- jest to niezbędne do osiągnięcia prawnie usprawiedliwionych celów administratora danych.

§ 6

Przetwarzanie danych osobowych w **W&H Sp. z. o.o. ul. Kościuszki 49 44-351 Turza Śląska** jest dozwolone wyłącznie pod warunkiem przestrzegania przepisów ustawy, aktów wykonawczych wydanych na podstawie ustawy oraz przepisów wydanych przez administratora danych – w szczególności Polityki i Instrukcji.

ROZDZIAŁ II
System ochrony danych osobowych

§ 7

Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych na poziomie podwyższonym/wysokim - w szczególności zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 8

- Administrator danych może powołać Administratora Bezpieczeństwa Informacji.
- Do zadań Administratora Bezpieczeństwa Informacji należy:
- zapewnianie przestrzegania przepisów o ochronie danych osobowych

sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych;

nadzorowanie aktualizowania Polityki i Instrukcji oraz przestrzegania zasad w nich określonych;

b) zapewnianie zapoznania użytkowników z przepisami o ochronie danych osobowych;

prowadzenie rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów, o których mowa w art. 43 ust. 1 ustawy, zawierającego nazwę zbioru oraz informacje, o których mowa w art.41 ust. 1 pkt 2–4a i 7 ustawy.

- Administrator danych może powierzyć Administratorowi Bezpieczeństwa Informacji wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań, o których mowa w u. 2.
- Wzór Powołania Administratora Bezpieczeństwa Informacji, wraz z zakresem dodatkowych obowiązków, o których mowa w u. 3, stanowi załącznik do Polityki.
- Administrator danych może stworzyć dodatkowe stanowiska związane z ochroną danych osobowych, w szczególności Administratora Systemów Informatycznych. Powołując osoby na stanowiska, o których mowa w zdaniu poprzedzającym, administrator danych określa zakres ich obowiązków i uprawnienia wobec użytkowników.

§ 9

- Administrator danych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej na piśmie, która określa zakres i cel przetwarzania danych.
- Umowa, o której mowa w ustępie poprzedzającym, musi zawierać zapewnienie podmiotu, któremu powierza się dane osobowe do przetwarzania, iż przed rozpoczęciem tego przetwarzania podejmie on środki zabezpieczające zbiór danych, o których mowa w art. 36-39 ustawy oraz, że spełni wymogi określone w art. 39a ustawy.

§ 10

- Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie nadane przez administratora danych (użytkownicy), które określa zakres i cel przetwarzania danych. Upoważnienie jest wydawane na czas określony lub nieokreślony. Wzór upoważnienia stanowi załącznik do Polityki.
- Administrator danych prowadzi Ewidencję osób upoważnionych do przetwarzania danych osobowych, w której wskazane jest imię i nazwisko osoby upoważnionej, identyfikator użytkownika, data nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych. Wzór ewidencji stanowi załącznik do Polityki.
- Użytkownicy są obowiązani zachować w tajemnicy przetwarzane przez nich dane osobowe oraz sposoby ich zabezpieczenia. W celu zabezpieczenia tego obowiązku potencjalny użytkownik, wraz z otrzymaniem zgody na przetwarzanie danych, podpisuje Oświadczenie o poufności.
- Administrator nie udziela upoważnienia do przetwarzania danych, jeśli potencjalny użytkownik odmówił podpisania Oświadczenia o poufności.
- Administrator danych może w każdym momencie cofnąć udzielone upoważnienie co odnotowuje w ewidencji, o której mowa w u. 2.
- Administrator danych zapewni, że osoby nieuprawnione nie uzyskają dostępu do danych osobowych przetwarzanych w organizacji, w szczególności uniemożliwi przetwarzanie danych osobowych podmiotom, którym nie udzielono upoważnienia, których upoważnienie wygasło lub zostało cofnięte.
- W celu realizacji obowiązku, o którym mowa w u. 6, administrator danych:
- udostępnia identyfikatory i hasła umożliwiające korzystanie z systemu informatycznego wyłącznie osobom posiadającym pisemne upoważnienie do przetwarzania danych osobowych;
- udostępnia klucze do budynków, pomieszczeń, szaf, sejfów itp., w których przechowywane są nośniki danych osobowych, wyłącznie osobom posiadającym pisemne upoważnienie do przetwarzania danych osobowych;
- niezwłocznie po wygaśnięciu lub cofnięciu użytkownikowi upoważnienia do przetwarzania danych osobowych administrator danych usuwa z systemu informatycznego jego identyfikator oraz odbiera mu klucze do obiektów, o których mowa w punkcie b;
- podejmie inne niezbędne i celowe środki, w szczególności może zastosować monitoring video, wprowadzić ewidencję wydawania kluczy, przechowywać nośniki danych osobowych w szafie stalowej lub zamykanych szafkach.

§ 11

- Użytkownicy mogą zbierać dane osobowe wyłącznie w zakresie adekwatnym ze względu na wykonywaną działalności, rodzaj i wartość transakcji, uzasadniony interes lub cel przetwarzania danych.
- Użytkownik zbierając dane jest obowiązany dopełnić obowiązki informacyjne, o których mowa w art. 24 i 25 ustawy, w szczególności poinformować osobę, od której zbiera dane, o celach tego działania.
- Dane osobowe mogą być zbierane wyłącznie z wiarygodnych źródeł.

- Użytkownik, niezwłocznie po powzięciu informacji o potrzebie aktualizacji danych osobowych, dokonuje takiej aktualizacji lub przekazuje informacje o potrzebie aktualizacji administratorowi danych, jeśli sam nie jest uprawniony do jej dokonania.

§ 12

- Użytkownik, niezwłocznie po zebraniu danych osobowych, wprowadza je do odpowiedniego zbioru danych, odnotowując w ewidencji lub systemie, o których mowa w u. 3 cel ich przetwarzania. Jeśli dane osobowe nie są wprowadzane do zbioru danych, należy odnotować, obok danych, cel ich zebrania.
- Użytkownik nie może przetwarzać danych w innych celach, niż te dla których zostały zebrane i odnotowane w sposób określony w u.1.
- Administrator danych zapewnia kontrolę nad tym jakie dane osobowe, kiedy i przez kogo zostały do zbioru danych wprowadzone oraz komu są przekazywane, poprzez zastosowanie następujących środków:
- w wypadku przetwarzania danych osobowych poza systemem informatycznym – prowadzony jest pisemny/elektroniczny rejestr, w którym każdy użytkownik, niezwłocznie po wprowadzeniu danych osobowych do zbioru lub ich przekazaniu, zamieszcza informacje o tym fakcie wraz z podaniem swojego imienia i nazwiska, daty dokonania tych czynności oraz zakresu wprowadzonych lub przekazanych danych osobowych; w wypadku przekazywania danych osobowych użytkownik zamieszcza również informację o tym komu zostały przekazane;
- w wypadku przetwarzania danych osobowych w systemie informatycznym – system ten zapewnia odnotowanie:
- daty pierwszego wprowadzenia danych do systemu – automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych;
- identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych ma wyłącznie jedna osoba – automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych;
- źródła danych w przypadku zbierania danych nie od osoby, której one dotyczą; jeżeli jednak dane osobowe zostały zebrane bezpośrednio od osoby, której dane dotyczą, system umożliwia odnotowanie tej okoliczności, chyba że wszystkie dane osobowe przetwarzane w danym zbiorze zostały zebrane bezpośrednio;
- informacji o odbiorcach danych (art. 7 pkt 6 ustawy) oraz innych osobach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
- sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8.
- Przepisy ustępu 3b nie muszą być stosowane, gdy system informatyczny służy wyłącznie do przetwarzania danych poprzez edycję tekstu, w celu udostępnienia danych na piśmie.

§ 13

Dane osobowe są przechowywane nie dłużej niż jest to niezbędne do osiągnięcia celów przetwarzania, określonych i odnotowanych zgodnie z § 11. Jeśli cele przetwarzania zostały osiągnięte, użytkownik niezwłocznie usuwa dane ze wszystkich zbiorów danych oraz innych miejsc, w których dane osobowe są przechowywane.

§ 14

Procedury wykonywania oraz rejestrowania naprawy, przeglądów i konserwacji systemów informatycznych oraz nośników służących do przetwarzania danych określa Instrukcja.

§ 15

- Użytkownicy, w wypadku zidentyfikowania faktu naruszenia systemu ochrony danych osobowych, w szczególności Polityki, są zobowiązani niezwłocznie powiadomić o tym administratora danych oraz podjąć czynności niezbędne do zminimalizowania skutków naruszenia i przywrócenia stanu zgodnego z przepisami, w szczególności:
- ustalić przyczynę i zakres naruszenia oraz osobę odpowiedzialną za jego powstanie;
- zabezpieczyć miejsce, w którym naruszenie powstało;
- rozważyć zaprzestanie przetwarzania danych osobowych, w tym w systemie informatycznym, do momentu ustalenia istotnych okoliczności naruszenia;
- zaniechać działań mogących utrudnić analizę zdarzenia.
- Przez naruszenie systemu ochrony danych należy rozumieć w szczególności:
- awarię jakiegokolwiek elementu systemu informatycznego;
- ostrzeżenie systemu antywirusowego o infekcji jakiegokolwiek elementu systemu informatycznemu;
- zaistnienie stanu zagrożenia dla pomieszczeń, w których przetwarzane są dane osobowe m.in. pożar, zalanie, zawalenie;
- przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe, których zachowanie wskazuje na próbę uzyskania nieuprawnionego dostępu do danych osobowych;
- utratę kopii zapasowych;
- nieuprawnione logowanie do systemu informatycznego;
- zniszczenie lub uszkodzenie jakiegokolwiek elementu systemu informatycznego
- Każde zgłoszenie naruszenia systemu ochrony danych osobowych jest rejestrowane przez administratora danych w Rejestrze Naruszeń, który stanowi załącznik do Polityki. Zgłoszenie zawiera krótki opis, przyczynę i zakres naruszenia oraz sposób postępowania na wypadek powstania podobnych stanów w przyszłości.

§ 16

- Administrator danych przybywa na miejsce naruszenia w celu zapoznania się z okolicznościami naruszenia i podjęcia decyzji co do dalszego postępowania, w szczególności ocenia zasadność wezwania specjalistów ds. systemów informatycznych.
- Jeśli zaprzestano przetwarzania danych osobowych, o jego wznowieniu decyduje administrator danych, chyba że ze względu na szczególne okoliczności konieczne jest natychmiastowe wznowienie ich przetwarzania.
- Użytkownik, który zgłosił naruszenie, jest zobowiązany do zrelacjonowania istotnych okoliczności naruszenia administratorowi danych. Administrator danych może również żądać wyjaśnień od innych osób, które mogą mieć wiadomości o zdarzeniu.

§ 17

- Administrator danych opracowuje i wdraża działania mające na celu przywrócenie bezpieczeństwa systemu ochrony danych osobowych oraz zabezpiecza system przed wystąpieniem podobnych stanów w przyszłości, w szczególności udziela niezbędnych pouczeń użytkownikom.
- Administrator danych może wydawać okresowe raporty dotyczące powstałych naruszeń i sposobów postępowania w celu ich zlikwidowania. Z raportami zobowiązani są zapoznać się wszyscy użytkownicy.

§ 18

- Użytkownikom zabrania się:
- przetwarzania danych osobowych w zakresie i celu niezgodnym z upoważnieniem lub przepisami prawa;
- udostępniania danych osobowych osobom nieupoważnionym do ich przetwarzania;
- wynoszenia urządzeń, na których przechowywane są dane osobowe, poza obszar przetwarzania danych osobowych;
- postępowania, przy przetwarzaniu danych osobowych, niezgodnego z porządkiem prawnym, Polityką i Instrukcją.
- Za nieprzestrzeganie zakazów i uchybienia w zakresie obowiązków dotyczących przetwarzania danych osobowych w organizacji grożą sankcje dyscyplinarne określone w Polityce.

§ 19

- Dane osobowe w organizacji przetwarzane są w budynkach, pomieszczeniach lub częściach pomieszczeń, tworzących obszar przetwarzania danych osobowych, które wyszczególnione są w załączniku nr 5 do Polityki.
- Użytkownicy nie mogą przetwarzać danych poza obszarem przetwarzania danych określonym w u. 1, w szczególności nie mogą wynosić z niego nośników danych, oprócz sytuacji określonych w Polityce i Instrukcji związanych z naprawą i konserwacją nośników danych.

§ 20

- Wykaz zbiorów danych osobowych wraz ze wskazaniem programów i sprzętu zastosowanych do ich przetwarzania stanowi załącznik nr 6 do Polityki.
- Wszelkie zmiany w zakresie baz danych osobowych, oprogramowania i sprzętu służącego do ich przetwarzania wymagają niezwłocznej modyfikacji wykazu, o którym mowa w u.1, przez administratora danych.
- Użytkownicy nie mogą korzystać z systemu informatycznego z naruszeniem powiązań wynikających z wykazu, o którym mowa w u.1.

§ 21

W zbiorach danych w organizacji przetwarzane są dane osobowe w zakresie określonym poprzez wskazanie pól informacyjnych i powiązań między nimi w załączniku nr 7 do Polityki.

§ 22

- Sposób przepływu danych pomiędzy poszczególnymi systemami w organizacji jest określony w załączniku nr 8 do Polityki.
- W związku ze sposobem funkcjonowania i powiązaniami między systemami informatycznymi stosuje się środki bezpieczeństwa na poziomie, o których mowa w § 7 u.1.

§ 22

Dla zapewnienia przetwarzanym danym poufności, integralności i rozliczalności stosuje się, oprócz innych wskazanych w Polityce, następujące organizacyjne i techniczne środki bezpieczeństwa:

- Biuro zamykane na klucz
- Komputer zabezpieczony hasłem
- Użytkownik posiada login i hasło do systemu
- Wylogowanie z systemu po zakończonej pracy

ROZDZIAŁ III

Sankcje

§ 23

Za naruszenie zakazów lub niedopełnienie obowiązków w zakresie przetwarzania danych osobowych, użytkownikom grożą następujące sankcje:

- Upomnienie/naganna
- Potrącenie z wynagrodzenia

ROZDZIAŁ IV

Podnoszenie kwalifikacji

§ 24

- Administrator danych zapewnia użytkownikom dostęp do szkoleń z zakresu ochrony danych osobowych.
- Użytkownik nie rzadziej niż 12 miesięcy ma obowiązek odbyć szkolenie w celu podwyższenia kwalifikacji w zakresie ochrony danych osobowych.
- W wypadku znaczącej zmiany w prawie dot. ochrony danych osobowych, administrator danych ma obowiązek niezwłocznie zapewnić użytkownikowi dostęp do aktualnych przepisów i literatury dot. ochrony danych osobowych. W miarę możliwości organizuje lub zapewnia dla użytkowników szkolenie w celu aktualizacji ich wiedzy w zakresie ochrony danych osobowych.

§ 25

Przed udzieleniem potencjalnemu użytkownikowi upoważnienia do przetwarzania danych osobowych, administrator danych zapewnia mu dostęp do materiałów edukacyjnych z zakresu ochrony danych osobowych i w miarę możliwości zapewnia mu szkolenie w tym zakresie. W celu sprawdzenia wiedzy potencjalnego użytkownika administrator danych może przeprowadzić test kompetencyjny.

ROZDZIAŁ V

Postanowienia końcowe

§ 26

- Polityka wchodzi w życie z dniem ogłoszenia, a jej treść jest ogólnie dostępna do wglądu u administratora danych.
- Użytkownik zobowiązany jest złożyć oświadczenie, o tym, iż zapoznał się z przepisami ustawy, wydanymi na jej podstawie aktami wykonawczymi, obowiązującą Polityką oraz Instrukcją. Wzór oświadczenia stanowi załącznik do Polityki.
- Wszelkie dokumenty, w tym załączniki do Polityki, związane z ochroną danych osobowych w organizacji przechowywane są przez administratora danych. Oświadczenia, upoważnienia i inne dokumenty dotyczące bezpośrednio danego użytkownika są przechowywane również w jego aktach osobowych.