P O L I T Y K A B E Z P I E C Z E Ń S T W A

Ochrony Danych Osobowych

Przedsiębiorstwo Produkcyjno – Handlowe ″WR″ spółka z o.o. z siedzibą w Przasnyszu

Polityka Bezpieczeństwa przyjęta Uchwałą Zarządu Nr 1/2018 r.
w dniu 25.05.2018 r.

WPROWADZENIE

Ochrona danych osobowych zawsze była traktowana jako jeden z najważniejszych aspektów w działalności Przedsiębiorstwa Produkcyjno – Handlowego ″WR″ spółka z o.o. z siedzibą w Przasnyszu (dalej: Administrator, zamiennie WR). Jako osoba prawna prowadząca działalność działalność gospodarczą w przedmiocie produkcji wyrobów metalowych, plastikowych oraz wózków elektrycznych, czuje się ona szczególnie odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w związku z tą działalnością. Należy w tym miejscu zaznaczyć, że Spółka posiada Zintegrowany System Zarządzania Jakością i Środowiskiem – certyfikaty ISO 9001 i ISO 14001, które systematyzują i uzupełniają politykę jakości i bezpieczeństwa WR.

Niniejsza Polityka Bezpieczeństwa stanowi usystematyzowane zasady obowiązujące w Przedsiębiorstwie Produkcyjno – Handlowym ″WR″ spółka z o.o. z siedzibą w Przasnyszu, które mają na celu wprowadzenie zabezpieczeń i zintensyfikowanie ochrony odnoszącej się do danych osobowych. Celem jest również opracowanie zasad związanych z obowiązkami informacyjnymi osób fizycznych, których dane są przetwarzane. Polityka ma charakter sektorowy i została zorientowana na poszczególną działalność firmy.

Wprowadzenie niniejszej Polityki Bezpieczeństwa jest konieczne z uwagi na wejście w życie z dniem 25 maja 2018 r. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE („RODO”).

Ze względów powyższych należało wprowadzić rozwiązania techniczne i organizacyjne, które mają na celu usystematyzowanie dotychczasowej polityki związanej z ochroną danych osobowych, ale skorelowanej z Rozporządzeniem RODO. Polityka Bezpieczeństwa zawiera także wzory niezbędnych klauzul informacyjnych, umów o przetwarzanie danych osobowych, a także koniecznych upoważnień. Znajduje się tu również informacja o podstawie prawnej przetwarzania danych osobowych.

Spółka WR przeprowadziła niezbędną analizę ryzyka związaną z przetwarzaniem danych osobowych i na tej też podstawie wprowadzono rozwiązania konieczne, mające na celu jak największą ochrony przetwarzanych danych.

Działalność gospodarcza spółki WR nie spełnia kryteriów przewidzianych w art. 37 ust. 1 lit. a,b,c Rozporządzenia RODO, a zatem nie ma obowiązku powoływania Inspektora Ochrony Danych Osobowych. Nie przetwarza także w swojej działalności danych osobowych na dużą skalę. Wobec powyższego odstąpiono od powoływania takiej osoby w Zakładzie Pracy.

Przepisy ogólne

§ 1.

1. Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych. Art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) stanowią, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących.

2. Zasady i przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych nie mogą - niezależnie od obywatelstwa czy miejsca zamieszkania takich osób - naruszać ich podstawowych praw i wolności, w szczególności prawa do ochrony danych osobowych. Wprowadzone niniejszą Polityką zasady mają na celu przyczyniać się do tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości.

§ 2.

1. Polityka Bezpieczeństwa ma zastosowanie na terenie zakładu pracy spółki WR, a także poza nim, jeżeli w związku z tą działalnością przetwarzane są dane osobowe (zakres terytorialny), nie jest ograniczona w czasie (zakres czasowy) i dotyczy wszystkich jej pracowników i współpracowników, bez względu na łączący ze spółką WR stosunek prawny (zakres podmiotowy).

2. Polityka Bezpieczeństwa reguluje prawa i obowiązki związane z przetwarzaniem danych osobowych w każdy sposób, bez względu na nazwę, rodzaj i cel przetwarzania, przy wykorzystaniu dostępnych, proporcjonalnych do zagrożeń środków organizacyjnych i technicznych służących ich ochronie.

3. Pracownicy spółki WR obowiązani są zapoznać się z niniejszą Polityką Bezpieczeństwa, a także ją stosować. Administrator udostępni każdemu pracownikowi jej egzemplarz do swobodnego wglądu, a Pracownik po zapoznaniu się z jej treścią podpisze pisemne oświadczenie (do akt osobowych), iż z niniejszą Polityką się zapoznał.

4. Polityka dostępna będzie do swobodnego wglądu w Zakładzie Pracy. Stanowi ona także źródło wiedzy dla organów kontrolnych przestrzegania przepisów odnoszących się do ochrony danych osobowych.

§ 3. Definicje

Definicje użyte w Polityce Bezpieczeństwa oznaczają:

a) **Administrator:** Przedsiębiorstwo Produkcyjno – Handlowe ″WR″ spółka z o.o. z siedzibą w Przasnyszu, ul. Leszno 59, 06-300 Przasnysz, KRS: 0000150227, NIP: 7611456543, kontakt: info@pphwr.com.pl, tel/fax.: 29 752 5463.
b) **Dane osobowe:** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

c) **Osobie, której dane dotyczą;** możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

d) **Przetwarzanie:** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

e) **Pseudonimizacja:** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

f) **Zbiór danych:** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

g) **Zakład pracy:** oznacza nieruchomość w której prowadzona jest działalność gospodarcza spółki WR, **,** adres: ulica Leszno 59, 06-300 Przasnysz.

h) **Podmiot przetwarzający**; oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

i) **Odbiorca**: oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

j) **Strona trzecia:** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które - z upoważnienia administratora lub podmiotu przetwarzającego - mogą przetwarzać dane osobowe;

k) **Zgoda:** osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

l) **Polityka** – oznacza niniejszą Politykę Bezpieczeństwa Ochrony Danych Osobowych.

§ 3.

1. Administrator odpowiada za przetwarzanie danych zgodnie z prawem. Dane osobowe muszą być:
a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość");
b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych");
d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("prawidłowość");
e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy,
f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ("integralność i poufność").

2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie (rozliczalność).

§ 4.

Administrator nie przetwarza danych osobowych osób małoletnich w rozumieniu Rozporządzenia RODO, nie dokonuje profilowania danych, ani nie posiada środków technicznych służących do automatyzowania danych osobowych poprzez ich systematyzowanie i przypisywanie do odpowiednich grup czy zdarzeń.

§ 5. Upoważnienie

1. Administrator mając na względzie różne sfery własnej działalności odrębnie
a) wyda Pracownikom pisemne upoważnienia do przetwarzania danych osobowych w działalności związanej z kadrowością i księgowością,
b) wyda Pracownikom pisemne upoważnienia do przetwarzania danych osobowych odnoszących się do pozostałej działalności WR, jeżeli pracownicy będą mieli styczność z danymi osobowymi.
2. Upoważnienie precyzyjnie będzie określać zbiór danych do którego poszczególny Pracownik będzie miał dostęp. Wzór upoważnienia stanowi załącznik nr 1.
3. Każdy pracownik obowiązany jest podpisać upoważnienie, które następnie złożone będzie do akt pracowniczych.

§ 6. Obsługa księgowa

Obsługę księgową i kadrową prowadzą pracownicy Spółki WR.

§ 7. Obsługa IT

Administrator w sytuacji korzystania z zewnętrznych zasobów IT, obowiązany jest do zawarcia dodatkowej Umowy o powierzenie przetwarzania danych osobowych. Administrator będzie korzystał z usług IT przedsiębiorców dających rękojmię należytej ochrony danych osobowych.

§ 8. Szkolenia RODO

Administrator w miarę swoich możliwości finansowych zleci przeprowadzenie na rzecz Pracowników szkolenia z zakresu ochrony danych osobowych.

§ 9. Przetwarzanie danych osobowych

1. Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.
2. Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie tych zasad nie jest wiążąca.
3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.
4. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

§ 10. Obowiązki informacyjne

1. Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą, wszelkich informacji związanych z przetwarzanymi danymi osobowymi oraz prowadzić z nią wszelką komunikację w sprawie przetwarzania. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach - elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.
2. Administrator ułatwia osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy niniejszej Polityki Bezpieczeństwa i Rozporządzenia RODO.
3. Administrator bez zbędnej zwłoki - a w każdym razie w terminie miesiąca od otrzymania żądania - udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem odnoszącym się do danych osobowych osoby wnioskującej. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter

żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.
4. Jeżeli administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie - najpóźniej w terminie miesiąca od otrzymania żądania - informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.
5. Informacje udzielane przez administratora w związku z zapytaniem odnoszącym się do ochrony danych osobowych są wolne od opłat.

Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:

a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo
b) odmówić podjęcia działań w związku z żądaniem.

Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

6. Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

§ 11.

1. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:
a) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
b) gdy ma to zastosowanie - dane kontaktowe inspektora ochrony danych;
c) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
d) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
e) gdy ma to zastosowanie - informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.
2. Poza informacjami, o których mowa w ust. 1, podczas pozyskiwania danych osobowych administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:
a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

b) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
c) informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
d) informacje o prawie wniesienia skargi do organu nadzorczego;
e) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
3. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2.

§ 12.

1. Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, administrator podaje osobie, której dane dotyczą, następujące informacje:
a) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
b) gdy ma to zastosowanie - dane kontaktowe inspektora ochrony danych;
c) cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania;
d) kategorie odnośnych danych osobowych;
e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
2. Poza informacjami, o których mowa w ust. 1, administrator podaje osobie, której dane dotyczą, następujące informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania wobec osoby, której dane dotyczą:
a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
b) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO - prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
c) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
d) informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
e) informacje o prawie wniesienia skargi do organu nadzorczego;
f) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych;
3. Informacje, o których mowa w ust. 1 i 2, administrator podaje:

a) w rozsądnym terminie po pozyskaniu danych osobowych - najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
c) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy - najpóźniej przy ich pierwszym ujawnieniu.
4. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2.
5. Ust. 1- 4 nie mają zastosowania, gdy - i w zakresie, w jakim:
a) osoba, której dane dotyczą, dysponuje już tymi informacjami;
b) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie;
c) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub
d) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

§ 13.

1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:
a) cele przetwarzania;
b) kategorie odnośnych danych osobowych;
c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
f) informacje o prawie wniesienia skargi do organu nadzorczego;
g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą - wszelkie dostępne informacje o ich źródle;
3. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z

kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.
4. Prawo do uzyskania kopii, o której mowa w ust. 3, nie może niekorzystnie wpływać na prawa i wolności innych.

§ 14.

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

§ 15. Prawo do bycia zapomnianym

1. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
c) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania
d) dane osobowe były przetwarzane niezgodnie z prawem;

§ 16.

Administrator informuje o sprostowaniu lub usunięciu danych osobowych każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

§ 17. Zawiadamianie o naruszeniu danych osobowych

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.
3. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
4. Jeżeli - i w zakresie, w jakim - informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki
5. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

§ 18

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki jakie podjęto.
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

§ 19. Rejestr przetwarzania danych osobowych

1. Administrator, w tym w ramach upoważnienia Inspektor, prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają. W rejestrze tym zamieszcza się wszystkie następujące informacje:
a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie - przedstawiciela administratora oraz inspektora ochrony danych;
b) cele przetwarzania;

c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej,
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.
2. Każdy podmiot przetwarzający oraz - gdy ma to zastosowanie - przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierający następujące informacje:
a) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie - przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;
b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
c) gdy ma to zastosowanie -przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej,
d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.
3. Rejestry mają formę pisemną, w tym formę elektroniczną.
4. Administrator lub podmiot przetwarzający oraz - gdy ma to zastosowanie - przedstawiciel administratora lub podmiotu przetwarzającego udostępniają rejestr na żądanie organu nadzorczego.
5. Wzór takiego rejestru zawiera załącznik nr 3 do niniejszej Polityki Bezpieczeństwa.

§ 20. Rejestr naruszeń danych osobowych

Administrator prowadzi rejestr naruszeń danych osobowych w formie pisemnej i elektronicznej. Wzór zawiera załącznik nr 4.

§ 21.

Spółka WR w ramach prowadzonej działalności przetwarza dane osobowe kontrahentów będących osobami fizycznymi prowadzącymi jednoosobową działalność gospodarczą (dane firmy, NIP, adres), dane pracowników, a także dane osób aplikujących na stanowisko (rekrutacja).

§ 22.

1. Budynek w którym prowadzona jest działalność spółki WR jest monitorowany, a także wyposażony w system sygnalizacyjny włamania i napadu. Jest także pod stałą ochroną zewnętrznej firmy świadczącej usługi ochrony osób i mienia. Dostęp poza godzinami pracy osób trzecich jest niemożliwy.

2. Pracownicy mają dostęp na teren Zakładu Pracy wyłącznie w godzinach pracy.
3. Dane osobowe odnoszące się do kontrahentów przetrzymywane są w oddzielnym pomieszczeniu. Przetrzymywane są w segregatorach, zamknięte w szafkach.
4. Do pomieszczenia mogą mieć dostęp wyłącznie osoby upoważnione przez Zarząd.
5. Dokumenty zawierające dane osobowe nie mogą znajdować się w miejscu widocznym i ogólnodostępnym.
6. Obwoluta dokumentów nie powinna zawierać żadnych danych osobowych.
7. Pracownicy nie mają dostępu do danych osobowych innych pracowników, chyba że Zarząd spółki WR pracowników do tych danych upoważni.
8. Monitory komputerów nie powinny być usytuowane w sposób umożliwiający zapoznanie się osobom trzecich z treścią widoczną na ekranie.
9. Dostęp do programów informatycznych jest przyznany indywidualnie.
10. Hasło do programów informatycznych zawiera znaki specjalne, duże litery i cyfry.

§ 23.

Dane kontrahentów spółki WR przechowywane są w odrębnym pomieszczeniu. Zasady przewidziane w § 22 należy stosować odpowiednio.

§ 24.

1. Budynek w którym prowadzona jest działalność wydawcza jest alarmowany.
2. Zaleca się, aby monitory komputerów przenośnych nie były skierowane na widok interesantów. W czasie obecności Interesantów na biurku nie mogą znajdować się dane, które identyfikowałyby jakiekolwiek dane osobowe.
3. Wszelkie dokumenty powinny być zabezpieczone i usystematyzowane w przeznaczonych specjalnie do tego szafkach. Dostęp do tych szafek mają wyłącznie upoważnieni pracownicy.
4. Sieć internetowa w Zakładzie Pracy jest zabezpieczona hasłem. Nie ma możliwości bez jego nieznajomości podłączenia się do sieci. Dostęp do Internetu mają wyłącznie upoważnieni pracownicy.
5. Zakazuje się korzystania z prywatnym skrzynek pocztowych na komputerach służących do pracy.
6. Segregatory jeżeli znajdują się na wierzchu, winny być zanonimizowane lub pseudonimizowane.
7. Dostęp Interesantów do pomieszczeń i szaf w których znajdują się dokumenty jest zabroniony.
8. Każdy pracownik ma zabezpieczony hasłem i profilowany dostęp do komputerów służących do wykonywania czynności zawodowych.

§ 25.

1. Administrator wydaje pracownikom stosowne upoważnienia do przetwarzania w Zakładzie Pracy danych osobowych.
2. W upoważnieniu określa się cel przetwarzania, ich zakres, a także okres na jaki upoważnienie zostało wydane. Treść upoważnienia winna być zgodna z przepisami Rozporządzenia RODO.

3. Upoważnienie składa się do akt osobowych pracownika. Pracownik jest zaznajomiony z przepisami niniejszej Polityki Bezpieczeństwa, a także Rozporządzenia RODO i innych przepisów powszechnie obowiązujących w zakresie obowiązku poprawnego przetwarzania danych osobowych.
4. Upoważnienia o których mowa wyżej różnią się celem i zakresem dla jakich zostały wydane.

§ 26

Dostęp do pomieszczeń w których przetwarzane są dane osobowe po zakończeniu godzin pracy jest niemożliwy, chyba że za uprzednią zgodą Administratora.

§ 26. POZOSTALI ODBIORCY

Administrator mając na względzie uzasadniony prawnie interes może przekazać dane osobowe Odbiorcom, ale tylko wyłącznie na podstawie zawartej umowy, która w sposób należyty i zgodny z przepisami Rozporządzenia RODO zabezpieczy dane osobowe. Jednakże cel takiego przekazania musi być prawnie uzasadniony i doprecyzowany w umowie. W miarę technicznych możliwości i uzasadnienia prawnego i faktycznego, Administrator powinien poinformować o takiej czynności osoby fizyczne, których dane przetwarza.

Przekazanie może nastąpić wyłącznie:
- radcy prawnemu (w związku z obsługą prawną i realizacji uzasadnionych prawnie interesów Administratora)
- Poczcie Polskiej S.A. (w związku z obsługą korespondencji),
- usługobiorcy IT (w związku z koniecznością wprowadzenia ulepszeń informatycznych, usunięcia bądź minimalizacji awarii czy wprowadzenia dodatkowych zabezpieczeń).

§ 27

1. Każdy upoważniony pracownik ma obowiązek w sposób szczególny chronić dane osobowe przetwarzane i gromadzone przez Administratora. Wiąże się z tym także konieczność minimalizacji danych, a także ich pseudonimizacji, w taki sposób, aby inne osoby nie miały do nich dostępu. Szczególnej ochronie podlegają wiadomości kierowane za pośrednictwem systemów komunikowania elektronicznego. Dane te winny być usystematyzowane i zabezpieczone z wyłączeniem dostępu osób trzecich. Każdy upoważniony winien logować się do systemów indywidualnie za pośrednictwem własnego loginu i rejestrować w rejestrze czynności takie logowanie wraz z informacją o przetwarzaniu danych.
2. Administrator w razie wątpliwości konsultuje czynności związane z przetwarzaniem danych osobowych z radcą prawnym bądź adwokatem.

§ 28.

W sprawach nieuregulowanych niniejszą Polityką Bezpieczeństwa zastosowanie będą miały przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, a także innych przepisów powszechnie obowiązujących.