POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

W

W & W NIERUCHOMOŚCI A. WÓJCIK, J. WÓJCIK SPÓŁKA JAWNA

Z SIEDZIBĄ W GLIWICACH

Zatwierdzam:

Data: 25.05.2018 r.

Podpis: .....

WŁAŚCICIEL

dr inż. Janusz Wójcik

Spis treści

§ 1. CELE POLITYKI BEZPIECZEŃSTWA

§ 2. DEFINICJE

§ 3. ZASIĘG ORAZ ZAKRES OBOWIĄZYWANIA POLITYKI

§ 4. ZASADY OGÓLNE PRZETWARZANIA DANYCH OSOBOWYCH

§ 5. BEZPIECZEŃSTWO DANYCH OSOBOWYCH

§ 6. OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH

§ 7. ORGANIZACJA PRACY PRZY PRZETWARZANIU DANYCH

§ 8. KONTAKT Z OSOBAMI, KTÓRYCH DANE DOTYCZĄ

§ 9. REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

§ 10. ZADANIA OSÓB ODPOWIEDZIALNYCH ZA OCHRONĘ DANYCH

§ 11. ODBIORCY DANYCH

§ 12. POSTĘPOWANIE Z INCYDENTAMI

§ 13. ODPOWIEDZIALNOŚĆ

ZAŁĄCZNIK NR 1. Rejestr Czynności Przetwarzania

ZAŁĄCZNIK NR 2. Wytyczne dotyczące oceny skutków dla ochrony danych

ZAŁĄCZNIK NR 3. Wzór upoważnienia

ZAŁĄCZNIK NR 4. Rejestr upoważnionych

§ 1. CELE POLITYKI BEZPIECZEŃSTWA

1. Polityka Bezpieczeństwa Danych Osobowych (dalej: **Polityka**) dotyczy danych osobowych przetwarzanych w **W & W Nieruchomości A. Wójcik, J. Wójcik Spółka Jawna** z siedzibą w Gliwicach, zwanej dalej również **Spółką** i opisuje stosowane przez Spółkę środki organizacyjne i techniczne, nakierowane na zapewnienie zgodności z prawem, rzetelności i przejrzystości, celowości procesów przetwarzania danych osobowych. Polityka opisuje także sposób realizacji zasady ograniczenia celu przetwarzania danych osobowych, minimalizacji zakresu zbieranych danych, utrzymania ich prawidłowości, ograniczenia czasowego przetwarzania oraz zapewnienia ich poufności i integralności. Realizacja powyższych zasad jest kluczowa dla prawidłowego zarządzania danymi osobowymi w Spółce.

2. Polityka, wraz z Instrukcją Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych (dalej: **Instrukcja**) ma stanowić zespół wytycznych, które osoby mające dostęp do danych osobowych przetwarzanych w Spółce winny przestrzegać. Dotyczy to w szczególności naszych pracowników, ale także innych osób, które otrzymują dostęp do danych osobowych, których jesteśmy administratorem

3. Postanowienia Polityki pozostają w zgodzie z postanowieniami zawartymi w:
    1) Konstytucji Rzeczpospolitej Polski z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483), ze szczególnym uwzględnieniem postanowień artykułów 47 i 51,
    2) Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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 (ogólne rozporządzenie o ochronie danych, dalej: **RODO**).
    3) Aktualnej w chwili wprowadzenia niniejszego dokumenty Ustawy o ochronie danych osobowych.

Przestrzeganie postanowień Polityki i Instrukcji nie zwalania osób je stosujących z działania w zgodzie z wyżej wskazanymi przepisami prawa, w zakresie, w jakim rozszerzają one postanowienia tu zawarte.

§ 2. DEFINICJE

Na potrzeby niniejszej Polityki, a także Załączników, wskazanym poniżej terminom nadaje się następujące znaczenie:

1) **„Administrator danych osobowych"**, **„Administrator"**, **„Spółka"**, **„my"**– W & W Nieruchomości A. Wójcik, J. Wójcik Spółka Jawna z siedzibą w Gliwicach, ul. Kozielska 490, 44-164 Gliwice, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS: 0000426110, posiadająca numer NIP: 9691522489 oraz REGON: 240913051;
2) **„Administrator Sieci Informatycznej"**, **„ASI"** – osoba odpowiedzialna za zarządzanie systemem informatycznym, w którym przetwarzane są dane osobowe i odpowiadająca za jego sprawne działanie; Zaznacza się, iż w przypadku braku powołania ASI, Administrator wyznacza osobę lub podmiot, który w ramach swoich zadań wykonuje zadania przypisane ASI;
3) **„dane osobowe"** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (**„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;
4) **„Inspektor Ochrony Danych"**, **„IOD"** - osoba fizyczna wyznaczona przez Administratora danych osobowych, która sprawuje nadzór nad przestrzeganiem zasad ochrony wynikających z RODO, innych przepisów Unii Europejskiej lub przepisów krajowych o ochronie danych i zobowiązana jest prowadzić dokumentację wynikającą z tychże przepisów, przy czym IOD jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO. W przypadku braku powołania IOD, przez Inspektora Ochrony Danych rozumie się osobę fizyczną wyznaczoną przez Administratora, która w ramach swoich obowiązków wykonuje zadania przypisane IOD w niniejszej Polityce;
5) **„profilowanie"** - dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
6) **„pseudonimizacja"** - 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;
7) **„przetwarzanie danych osobowych"**, **„przetwarzanie"** – każda operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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;

8) **„Ustawa"** – obowiązująca w chwili wprowadzenia niniejszej polityki ustawa o ochronie danych osobowych;
9) **„zbiór danych osobowych"**, **„zbiór"** – każdy uporządkowany zestaw danych osobowych, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie; zbiór danych może być prowadzony zarówno w formie elektronicznej jak i papierowej.

§ 3. ZASIĘG ORAZ ZAKRES OBOWIĄZYWANIA POLITYKI

1. Celem niniejszej Polityki jest określenie zasad przetwarzania danych osobowych oraz ich bezpieczeństwa, jako zestaw praw, reguł, procedur i praktycznych doświadczeń regulujących sposób ich przetwarzania, zarządzania, ochrony i dystrybucji wewnątrz Spółki, jak i w kontaktach z otoczeniem.

2. Polityka wraz z Instrukcją opisują zabezpieczenia techniczne i organizacyjne, zastosowane celem ochrony danych osobowych w Spółce. Czyniąc zadość art. 30 RODO, w Spółce prowadzony jest Rejestr Czynności Przetwarzania, zgodny z Załącznikiem nr 1 do Polityki.

3. W związku z powyższym uznajemy za kluczowe, by wszystkie osoby zatrudnione w Spółce niezależnie od stosunku prawnego regulującego podstawę ich zatrudnienia, zapoznały się i przestrzegały postanowień tego dokumentu. Powyższe znajduje zastosowanie do osób posiadających chociażby przejściowy dostęp do danych, w tym niezależnych podwykonawców oraz osób, które realizują zadania w imieniu podwykonawców.

4. Polityka znajduje zastosowanie do wszelkich operacji, na danych osobowych, jakie mają miejsce w Spółce, w tym do:
    1) danych osobowych przetwarzanych w systemach informatycznych oraz w tradycyjnej - papierowej formie, a także przechowywanych na wszelkich nośnikach magnetycznych, optycznych, elektronicznych takich jak: zewnętrzny dysk, CD/DVD/Blue-Ray, pamięć USB;
    2) danych osobowych przetwarzanych zarówno w zbiorach danych, zestawach oraz pojedynczych informacjach osobowych,
    3) informacji dotyczących bezpieczeństwa danych osobowych, w szczególności informacji służących do uwierzytelnienia się w systemach informatycznych, w których mogą występować dane osobowe (loginy i hasła).

5. Polityka znajduje zastosowanie do wszystkich lokalizacji – budynków i pomieszczeń – w których są lub będą przetwarzane dane, ale także do przetwarzania, które odbywa się na urządzeniach mobilnych, takich jak telefony komórkowe lub laptopy. W formie stacjonarnej przetwarzanie odbywa się w siedzibie Spółki.

   Niniejsza Polityka jest udostępniana w formie elektronicznej, bądź w siedzibie Spółki, na wniosek osób, które zostały przez nas upoważnione do przetwarzania danych osobowych. Ponadto Polityka jest przekazywana każdorazowo osobie, która takie upoważnienie ma dostać.

§ 4. ZASADY OGÓLNE PRZETWARZANIA DANYCH OSOBOWYCH

1. Rodzaj działalności prowadzonych przez firmy, w tym przez Spółkę, powoduje, iż ma ona dostęp do szeregu danych osobowych. Wszelkie dane osobowe, w których posiadanie wejdzie Spółka, winny być przez nas należycie chronione, a stosowane przez nas środki ochrony tych danych odpowiadać powinny m.in. wymaganiom wynikającym z RODO.

2. Jako Spółka jesteśmy świadomi, iż dane przetwarzane są przez nas na niemal każdym etapie naszej działalności. Dane osobowe pozyskujemy przede wszystkim od pracowników firm. Niezależnie od tego przetwarzamy jednak dane osobowe naszych kontrahentów, pracowników, współpracowników, etc.

3. Z uwagi na rodzaj prowadzonej działalności, zmuszeni jesteśmy również udostępniać dane osobowe podmiotom trzecim.

4. Niniejsza Polityka ma więc na uwadze cel przetwarzania danych osobowych wykonywany przez Spółkę, jakim jest przede wszystkim właściwe realizowanie zadań gospodarczych Spółki.

5. Naszą intencją jest, by przetwarzanie w Spółce danych osobowych odbywało się za aprobatą wszystkich podmiotów, których dane dotyczą, w sposób transparentny i rzetelny.

6. Wszystkie dane osobowe gromadzone w Spółce mogą być przetwarzane wyłącznie w sposób zgodny z przepisami prawa. Dane przetwarzane mogą być jedynie, jeśli spełniona jest jedna z przesłanek, wymienionych w art. 6 ust. 1 RODO.

7. W działalności Spółki przewidujemy, iż spośród przesłanek wymienionych w tym przepisie, dane osobowe mogą być przetwarzane najczęściej na podstawie tych wskazanych w literach a), b), c) oraz f). Konsekwentnie, jeśli w naszym imieniu przetwarzasz dane osobowe, upewnij się, że występuje co najmniej jedna z tych okoliczności:
    1) osoba, której dane dotyczą wyraziła zgodę na takie przetwarzanie danych osobowych,
    2) przetwarzanie danych jest niezbędne, w celu wykonania umowy wiążącej nas z osobą, której dane dotyczą lub w celu zawarcia z nią takiej umowy na jej własne żądanie,
    3) przetwarzanie takich danych jest niezbędne, by Spółka zrealizowała ciążący na niej obowiązek prawny,
    4) istnieje prawnie uzasadniony interes Spółki lub innego podmiotu w przetwarzaniu tych danych, wcześniej przeanalizowany i zaakceptowany przez Zarząd.

    Jeśli masz wątpliwości, co do tego, czy przetwarzanie znajduje podstawę w którejś z wymienionych przesłanek, niezwłocznie poinformuj o tym bezpośredniego przełożonego lub IOD.

8. Zbierane dane powinny być merytorycznie poprawne, dlatego unikaj zbierania danych, o których wiesz, że są nieprawdziwe i w miarę możliwości ustalaj dane poprawne. Dążenie do ustalenia poprawnych danych powinno bezwzględnie odbywać się z poszanowaniem praw i

prywatności osób, których dane dotyczą oraz z uwzględnieniem zasady minimalizacji danych (nie zbierania przy tym danych dodatkowych).

9. Przy przetwarzaniu wszelkich danych osobowych, poza właściwą podstawą z art. 6 ust. 1 RODO należy zawsze mieć świadomość celu przetwarzania i ustalić, czy cel jest zgodny z ustaloną podstawą. Odrębne cele przetwarzania wymagają bowiem każdorazowo znalezienia prawidłowej podstawy przetwarzania danych osobowych.

10. Zabronione jest zbieranie jakichkolwiek danych nieistotnych z punktu widzenia celu przetwarzania lub o większym stopniu szczegółowości niż jest to potrzebne dla osiągnięcia tego celu. Jeśli więc jesteś odpowiedzialny za proces zbierania danych w związku z pewnym celem, upewnij się, że nie żądasz danych, które nie będą niezbędne do osiągniecia tego celu.

11. Dane mogą być przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania, w tym obejmujących cele Spółki takie jak dochodzenie roszczeń, czy obowiązki związane z archiwizacją dokumentów. Po tym okresie dane mogą być przechowywane tylko po uprzedniej ich anonimizacji.

12. Aby uchronić gromadzone przez Spółkę dane osobowe przed utratą, kradzieżą, bądź nieautoryzowanymi zmianami, wdrażamy szereg zabezpieczeń związanych z ich fizyczną ochroną oraz bezpieczeństwem w sferze informatycznej. Jest obowiązkiem każdej osoby upoważnionej do przetwarzania danych osobowych stosować się do przyjętych przez Spółkę zasad bezpieczeństwa.

13. Celem zapewnienia systemowego i kompleksowego podejścia do ochrony danych osobowych w Spółce, ustanowiliśmy Inspektora Ochrony Danych, z którym możesz skonsultować się w przypadku jakichkolwiek wątpliwości odnośnie stosowania niniejszej Polityki.

14. Spółka działa zgodnie z zasadą uwzględniania prywatności na etapie projektowania oraz prywatności jako ustawienia domyślnego. Te dwie zasady winny znaleźć odzwierciedlenie przy każdym nowym projekcie wdrażanym przez Spółkę i fakt ten powinien być udokumentowany.

15. W przypadku nowych projektów wdrażanych przez Spółkę, w tym przede wszystkim, jeśli przewidują one przetwarzanie danych osobowych w sferze elektronicznej, należy ocenić, jak projektowane rozwiązania będą wpływać na prawa i wolności osób, których dane dotyczą. W tym celu, każdorazowo zespół zajmujący się nowym projektem powinien zawierać w swoim składzie osobę, która będzie odpowiedzialna za bieżącą kontrolę tego, jak proponowane przedsięwzięcie wpłynie na bezpieczeństwo danych osobowych, które przetwarzamy, a także tych, które możemy przetwarzać w przyszłości.

16. Zapewnienie prywatności, jako ustawienia domyślnego oznacza, że naszą intencją jest minimalizacja przetwarzanych danych osobowych, a każdorazowe podanie danych osobowych przez osobę, której dane dotyczą, czy wyrażenie przez nią zgody na przetwarzanie tych danych,

musi wymagać wyraźnego potwierdzającego działania. Nieodpuszczalna jest sytuacja, kiedy do zbierania danych o osobie dochodzi bez jej wiedzy czy w sposób, w którym jest ona niepoinformowana o możliwości odmowy podania pewnych danych.

§ 5. BEZPIECZEŃSTWO DANYCH OSOBOWYCH

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, Spółka wdrożyła odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z przepisami prawa. Środki te opisane zostały w niniejszej Polityce oraz w Instrukcji. Środki te będą w razie potrzeby poddawane przeglądom i uaktualniane.

2. Zapewnienie bezpieczeństwa danych polega na zagwarantowaniu:
   1) **poufności danych,** tj. zapewnieniu, iż jedynie uprawnione osoby posiadać będą dostęp do danych – Spółka realizuje to wymaganie poprzez nadawanie upoważnień do przetwarzania danych osobowych - jeśli nie posiadasz upoważnienia do przetwarzania danych osobowych, a w ramach swoich obowiązków powinieneś przetwarzać takie dane, niezwłocznie zgłoś to bezpośredniemu przełożonemu;
   2) **integralności danych,** tj. dokładności oraz kompletności danych, jak również metod weryfikacji ich poprawności – Spółka realizuje tą wytyczną poprzez wdrożenie systemów informatycznych, które agregują dane i wymagają odpowiedniego stopnia autoryzacji do wykonywania operacji;
   3) **rozliczalności działań**, przez co należy rozumieć, że wszystkie działania istotne w zakresie przetwarzania danych zostały zarejestrowane, a w konsekwencji możliwe jest zidentyfikowanie osoby odpowiedzialnej za dokonanie konkretnej operacji na danych – w tym celu wszystkie operacje dokonywane w systemie informatycznym są dokonywane przez indywidualnie określone osoby – upewnij się, że używając systemów informatycznych korzystasz ze swojego własnego loginu i nie udostępniasz go innym;
   4) **dostępności danych,** czyli zapewnieniu dostępu do danych osobom, których dane dotyczą – Spółka wdraża zasady organizacyjne zapewniające osobom, których dane dotyczą wgląd do ich danych w określonym zakresie;
   5) **odporności systemów i usług przetwarzania,** czyli przedsięwzięciu działań zmierzających do uniemożliwienia bądź uodpornienia systemów informatycznych lub procesów przetwarzania na ataki z zewnątrz – Spółka utrzymuje oprogramowanie zapobiegające nieautoryzowanemu dostępowi do danych, a także podejmuje działania, aby wszelkie aplikacje, gdzie dane są przetwarzane, były na bieżąco aktualizowane;
   6) **prawidłowego zarządzenia ryzykiem**, tj. przedsięwzięciu działań zmierzających do umożliwienia zidentyfikowania, kontrolowania oraz eliminowania powstającego w związku z przetwarzaniem danych ryzyka naruszenia praw i wolności osób fizycznych – Spółka prowadzi okresowe szkolenia dla personelu, aby zapewnić, że jest świadoma ryzyk związanych z przetwarzaniem danych osobowych – jeśli czujesz, że pewne aspekty Twojej pracy w zakresie, w jakim przetwarzasz dane osobowe pozostają niejasne, w tym na przykład nie wiesz, w jaki sposób realizowane są w praktyce postanowienia niniejszej Polityki, skontaktuj się z bezpośrednim przełożonym lub Inspektorem Ochrony Danych.

3. Celem zapewnienia bezpieczeństwa danych osobowych wprowadzono mechanizmy ochronne, które wzajemnie się przenikają. Mechanizmami tymi są zabezpieczenia fizyczne, środki sprzętowe, procedury organizacyjne oraz rozwiązania informatyczne.

4. Zabezpieczenia **fizyczne** obejmują w szczególności:
   1) umożliwianie dostępu do danych osobowych tylko osobom, które posiadają ku temu stosowne upoważnienie,
   2) przechowywanie fizycznych zbiorów danych w szafkach/pomieszczeniach zamykanych na klucz, w tym dotyczy to serwerów, na których gromadzone są dane w formie elektronicznej,
   3) ochrona pomieszczeń, w których przechowywane są dane osobowe, przez podmiot zewnętrzny,
   4) stosowanie monitoringu.

5. Środki **sprzętowe** obejmują zwłaszcza:
   1) sprzęt wykorzystywany w ramach systemu informatycznego służącego do przetwarzania danych osobowych, zapewniający odpowiednie zabezpieczenia w zakresie dostępu do danych,
   2) przechowywanie danych osobowych na serwerach firm zewnętrznych, zapewniających najwyższe standardy zabezpieczenia danych osobowych, podparte odpowiednimi postanowieniami umownymi, które przewidują warunki przechowywania danych przez podmioty zewnętrzne,
   3) wykorzystanie niszczarki lub usług profesjonalnej firmy zajmującej się niszczeniem dokumentów do skutecznego usuwania dokumentów zawierających dane osobowe.

6. Procedury **organizacyjne** obejmują w szczególności:
   1) szkolenia dla pracowników mających dostęp do danych,
   2) okresowe audyty ochrony danych osobowych,
   3) przeprowadzanie oceny wpływu na przetwarzanie danych w przypadkach i zgodnie z procedurą opisaną w § 6.
   4) obowiązek dokładania ciągłych starań mających na celu zapewnienie zgodności ochrony danych z aktualnie obowiązującymi wymaganiami, w tym dostosowywania brzmienia Polityki i Instrukcji do zmieniającego się otoczenia prawnego,
   5) utworzenie funkcji Inspektora Ochrony Danych, który skupia wiedzę oraz kompetencje w obszarze ochrony danych osobowych.

7. Środki ochrony w ramach **rozwiązań informatycznych** polegają na:
   1) ograniczeniu identyfikatorem i hasłem dostępu do urządzeń i aplikacji, za pomocą których przetwarzane są dane,
   2) ograniczaniu dostępu użytkownika jedynie do konkretnych zasobów poprzez nadawanie im określonego zakresu uprawnień z poziomu administratora,
   3) stosowaniu programów mających na celu bieżące monitorowanie obecności złośliwego oprogramowania,

4) bieżącym aktualizowaniu używanego oprogramowania,
5) ochronie sieci lokalnej przed działaniami inicjowanymi z zewnątrz przy użyciu zapory sieciowej (firewall),
6) wykonywaniu kopii zapasowych.

§ 6. OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH

1. Na dzień wejścia w życie niniejszego dokumentu oceniamy, iż Spółka nie prowadzi procesów przetwarzania danych osobowych, które wymagałyby przeprowadzenia procedury oceny skutków dla ochrony danych osobowych, o której mowa w art. 35 RODO. Naszym obowiązkiem jest jednak na bieżąco badać, czy przesłanki tego przepisu są spełnione, tj. czy istnieje duże prawdopodobieństwo, że prowadzone przez Spółkę procesy przetwarzania danych osobowych mogą powodować wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, których dane dotyczą.

2. Przed rozpoczęciem nowego procesu przetwarzania danych osobowych lub zmiany procesu istniejącego, Spółka jest zobowiązana ustalić, czy nowy proces lub nowy sposób przetwarzania spełnia warunki, o których mowa w punkcie 1 i przez to wymaga przeprowadzenia oceny skutków dla ochrony danych osobowych.

3. Ustalenia tego dokonuje się poprzez zbadanie, czy w danym procesie przetwarzania dochodzi do **co najmniej dwóch czynności** z poniższej listy:
   1) ocena lub punktacja osób fizycznych, w tym ich profilowanie lub prognozowanie ich zachowań na podstawie zebranych danych osobowych;
   2) podejmowanie automatycznych decyzji mających skutki prawne lub w podobny sposób istotnie wpływających na sytuację osoby, której dane dotyczą;
   3) systematyczne monitorowanie, przez które rozumie się przetwarzanie danych w celu obserwowania, monitorowania lub kontroli osób, których dane dotyczą;
   4) przetwarzanie danych wrażliwych – pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, a także przetwarzanie danych dotyczących komunikacji elektronicznej, danych o lokalizacji czy danych finansowych;
   5) przetwarzanie danych na dużą skalę – pod względem liczby bezwzględnej osób, procentu populacji, zasięgu terytorialnego przetwarzania;
   6) porównywanie lub łączenie danych pochodzących z różnych zbiorów danych;
   7) przetwarzanie danych osób wymagających szczególnej ochrony np. pracowników, dzieci, pacjentów czy osób starszych;
   8) innowacyjne użycie lub zastosowanie technologicznych lub organizacyjnych rozwiązań, np. połączenie identyfikacji odciskiem palca oraz mechanizmu rozpoznawania twarzy w celu uzyskania dostępu do pomieszczeń; w zakres takiego przetwarzania wchodzą aplikacje mieszczące się w pojęciu "Internet of things";
   9) transgraniczny transfer danych poza Unię Europejską;
   10) przetwarzanie danych uniemożliwiające osobom, których dane dotyczą korzystanie z praw (np. monitoring obszarów publicznie dostępnych) lub mające na celu dopuszczenie do korzystanie z usługi lub zawarcia umowy.

4. Lista, o której mowa w punkcie 3 powyżej, ma służyć jako wytyczna, nawet bowiem, jeśli z innych niż wymienione tam powodów, osoby odpowiedzialne za wdrożenie nowej metody przetwarzania danych osobowych uznają, iż może rodzić ryzyko naruszenia praw i wolności osób, których dane dotyczą, powinny one przeprowadzić ocenę skutków dla ochrony danych osobowych zgodnie z punktami następnymi.

5. Ocenę skutków dla ochrony danych rozpoczyna zgłoszenie Inspektorowi Ochrony Danych przez osobę odpowiedzialną za dany projekt, potrzeby przeprowadzenia takiej oceny. Brak takiego zgłoszenia może stanowić istotne naruszenie obowiązków osoby koordynującej projekt.

6. Inspektor Ochrony Danych następnie decyduje, czy samodzielnie uczestniczyć w procesie oceny, czy też wyznaczyć osobę odpowiedzialną za proces lub w tym zakresie polegać na usługach podmiotu trzeciego (osoba lub podmiot tak wyznaczony zwany dalej: Koordynator DPIA) .

7. Niezależnie od wyboru, Koordynator DPIA zbiera informacje o projekcie, aby ustalić realne zagrożenia dla przetwarzanych danych osobowych, zbadać, jak te ryzyka mają być ograniczane i czy takie ograniczenia są skuteczne. Wszystkie osoby zaangażowane w projekt mają obowiązek współpracować z Koordynatorem DPIA, to jest udzielać mu informacji o merytorycznych założeniach projektu, które będą niezbędne by Koordynator wykonywał swoje obowiązki. Metodologia prac winna opierać się na kryteriach Grupy Roboczej Artykułu 29, które stanowią Załącznik nr 2 do Polityki.

8. Koordynator DPIA sporządza pisemny raport ze swoich prac, który obejmuje co najmniej:
   1) opis planowanych operacji przetwarzania i celów przetwarzania z rozróżnieniem na możliwe warianty projektu, jeśli są rozważane;
   2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne;
   3) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania oraz źródeł ryzyka;
   4) ocenę prawdopodobieństwa wystąpienia tego ryzyka;
   5) środki planowane w celu:
      a. zaradzenia ryzyku;
      b. wykazania przestrzegania przepisów, w tym RODO oraz niniejszej Polityki;
   6) ocenę, czy środki są skuteczne i wystarczające, by te cele osiągnąć, z uwzględnieniem indywidualnej oceny dla różnych wariantów, projektu, jeśli są rozważane.

9. Raport jest zatwierdzany przez Inspektora Ochrony Danych, a następnie przekazywany Zarządowi. W przypadku, jeśli władze Spółki uznają, że raport pozwala przyjąć, iż planowane środki są wystarczające, by zabezpieczyć prawa i wolności osób fizycznych w procesie przetwarzania, a także zapewnić zgodność z przepisami i niniejszą Polityką, proces może zostać wdrożony. W przeciwnym wypadku władze Spółki mogą zdecydować o zamknięciu projektu, a w szczególnie uzasadnionych przypadkach podjąć procedurę konsultacji z organem nadzoru, o której mowa w art. 36 RODO.

§ 7. ORGANIZACJA PRACY PRZY PRZETWARZANIU DANYCH

1. Będąc pracownikiem lub inną osobą dopuszczoną do przetwarzania danych osobowych, których Spółka jest administratorem, upewnij się że zapoznałeś się zasadami dotyczącymi bezpieczeństwa danych osobowych, a także, że otrzymałeś stosowne upoważnienia do przetwarzania tych danych; upoważnienia może przyznawać ADO lub osoba posiadająca pełnomocnictwo wydane przez ADO i, co do zasady, powinny być zgodne ze wzorem upoważnienia określonym w Załącznik nr 3 do Polityki. Upoważnienie może mieć formę pisemną, jak i elektroniczną.

2. Spółka prowadzi wykaz osób uprawnionych do przetwarzania danych osobowych zgodnie z Załącznikiem nr 4, osoby upoważnione nie są wykreślane z wykazu po ustaniu upoważnienia, a jedynie odnotowuje się w nim datę wygaśnięcia tego upoważnienia.

3. Każda osoba przetwarzająca dane osobowe, których administratorem jest Spółka, w czasie ich przetwarzania jest odpowiedzialna za ich bezpieczeństwo i w tym celu powinna ona dokładać wszelkich starań, celem uniemożliwienia wglądu bądź zmiany przetwarzanych danych przez osoby do tego nieupoważnione.

4. Osoby dopuszczone do przetwarzania danych są zobowiązane do zachowania w tajemnicy przetwarzanych danych osobowych.

5. Wszystkie osoby, o których mowa w punkcie 1 są zobowiązane do stosowania zasady *„czystego biurka"*. Oznacza to, że po zakończonej pracy lub przed opuszczeniem stanowiska pracy na dłuższy czas należy upewnić się, że:
   1) na stanowisku roboczym nie pozostały niezabezpieczone dokumenty z danymi osobowymi,
   2) szafy, w których przechowywane są dane osobowe zostały zamknięte w sposób uniemożliwiający dostęp osób, które nie są upoważnione do przetwarzania danego zakresu danych,
   3) komputer został doprowadzony do stanu, który przed wzbudzeniem będzie wymagał podania indywidualnego hasła użytkownika.

6. W miarę możliwości monitor komputera, na którym przetwarzane są dane osobowe powinien być ustawiony w ten sposób, by osoby, które nie mają dostępu do przetwarzania danego zakresu danych, w tym szczególnie osoby postronne, nie miały bezpośredniej możliwości obserwowania aktywności wykonywanej na tym monitorze.

7. W zakresie, w jakim jest to możliwe, pomieszczenia lub miejsca, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych.

8. **Wszelkie procesy przetwarzania danych osobowych, które odbywają się w Spółce powinny znaleźć odzwierciedlenie w Rejestrze Czynności Przetwarzania. Dlatego też zawsze upewnij się, że operacje, których dokonujesz na danych są objęte tym rejestrem. Jeśli masz jakiekolwiek wątpliwości w tym zakresie, skontaktuj się z Inspektorem Ochrony Danych.**

§ 8. KONTAKT Z OSOBAMI, KTÓRYCH DANE DOTYCZĄ

1. Naszym celem jest, by wszelka komunikacja z osobami, których dane dotyczą odbywała się w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

2. Informacji osobie, której dane dotyczą należy udzielać na piśmie lub elektronicznie, w zależności od jej wyboru. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość tej osoby.

3. W przypadku zbierania danych osobowych bezpośrednio od osób, których dane dotyczą (a wiec na przykład: na formularzach, umowach, kwestionariuszach, drukach, zarówno papierowych, jak i elektronicznych), należy umieszczać na nich klauzulę informacyjną, jeśli osoba ta nie dysponuje tymi danymi. Klauzula informacyjna winna być łatwo dostępna, widoczna, wyodrębniona od innych oświadczeń i zawierać:
   1) pełną nazwę i adres Spółki,
   2) imię, nazwisko i adres Inspektora Ochrony Danych, jeśli został ustanowiony,
   3) cel zbierania danych oraz podstawę ich przetwarzania, a jeśli podstawą jest prawnie uzasadniony interes Spółki (art. 6 ust. 1 lit. f) RODO), również informację na temat tego uzasadnionego interesu,
   4) okres, przez który dane osobowe będą przetwarzane, a jeśli nie jest to możliwe, kryteria ustalenia tego okresu,
   5) nazwy lub kategorie podmiotów, którym dane mogą być przekazywane,
   6) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także o prawie do przenoszenia danych, żądania ich usunięcia lub wniesienia sprzeciwu w sytuacjach prawem przewidzianych,
   7) jeżeli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
   8) informacje o prawie wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych,
   9) informacje czy podanie określonych danych jest obowiązkowe, czy też dobrowolne,
   10) w sytuacji, gdy podanie danych jest dobrowolne, informację czy jest ono niezbędne do podjęcia przez Spółkę określonych czynności, w tym, jakie są konsekwencje niepodania danych,
   11) w sytuacji, gdy podanie danych jest obowiązkowe, przepis prawa, który konstytuuje taki obowiązek,
   12) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu (jeśli dotyczy).

4. W przypadku zbierania danych osobowych z innych źródeł (nie od osoby, której dane dotyczą), bezpośrednio po utrwaleniu zebranych danych, nie później jednak niż w terminie 1 miesiąca od ich utrwalenia lub do momentu pierwszej komunikacji z osobą, której dane dotyczą

(którekolwiek nastąpi wcześniej), należy udzielić tej osobie informacji, o których mowa w ust. 9, z wyłączeniem pkt. 9-11, a ponadto również informacji o:

1) zakresie przetwarzanych danych (ich kategoriach);
2) źródle, z którego dane zostały pozyskane, w tym, czy pochodzą one ze źródeł powszechnie dostępnych;
3) prawach do wniesienia sprzeciwu w odniesieniu do przetwarzania danych osobowych, w zakresie wynikającym z art. 21 RODO.

5. Udzielenie informacji, o których mowa w punkcie 4 powyżej, nie jest obowiązkowe, jeżeli:
   1) osoba, której dane dotyczą dysponuje już tymi informacjami,
   2) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku,
   3) pozyskiwanie lub ujawnianie danych jest wyraźnie uregulowane prawem,
   4) Spółka jest w tym zakresie związana obowiązkiem zachowania w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej.

6. Jeżeli Spółka planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje ona osobę, której dane dotyczą, o tym innym celu. Powyższe nie może uchybiać postanowieniom dotyczącym istnienia podstawy prawnej dla każdego przetwarzania.

7. Do obowiązków każdej osoby dopuszczonej do przetwarzania danych w Spółce należy upewnienie się, że kontakt z osobą, której dane dotyczą odbywa się zgodnie z postanowieniami niniejszego paragrafu. Jeśli więc masz wątpliwości, czy osoby, których dane przetwarzasz otrzymały powyższe informacje, poinformuj o tym fakcie bezpośredniego przełożonego lub Inspektora Ochrony Danych.

§ 9. REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

1. Naszym obowiązkiem jest zapewnić osobom, których dane dotyczą przestrzeganie ich praw, przysługujących w związku z przetwarzaniem ich danych osobowych. Realizacja praw osób spoczywa na kierownikach poszczególnych projektów (czynności przetwarzania danych), którzy decydują o sposobie załatwienia wniosków osób fizycznych w tym zakresie, jednak w ramach naszej organizacji każda osoba, która przetwarza dane osobowe może spotkać się z takim wnioskiem, stąd też ważne, by zapoznać się z prawami, jakie osoby, których dane dotyczą mogą wykonywać.

2. Niniejszy paragraf opisuje kluczowe elementy związane z wykonywaniem praw osób, których dane dotyczą, jednak w przypadku realizacji takich praw przez te osoby wobec Spółki, osoby odpowiedzialne za ich realizację winny bezwzględnie stosować przepisy art. 16-22 RODO.

3. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych, a zwłaszcza prawo do:
    1) uzyskania wyczerpującej informacji o przetwarzaniu danych, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy,
    2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych,
    3) uzyskania informacji, od kiedy przetwarza się dane jej dotyczące, do kiedy planowane jest ich przetwarzanie oraz podania w powszechnie zrozumiałej formie treści tych danych,
    4) uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące, chyba że Administrator Danych Osobowych jest zobowiązany do zachowania w tym zakresie w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej,
    5) uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,
    6) uzyskania informacji o prawie wniesienia skargi do organu nadzorczego,
    7) uzyskania informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu,
    8) żądania sprostowania danych nieprawidłowych,
    9) żądania usunięcia dotyczących jej danych, jeśli wystąpiły okoliczności z art. 17 ust. 1 RODO (prawo do bycia zapomnianym),
    10) żądania ograniczenia przetwarzania, w przypadkach opisanych w art. 18 ust. 1 RODO,
    11) przenoszenia danych zgodnie z art. 20 RODO,
    12) gdy przetwarzanie danych odbywa się ze względu na prawnie uzasadniony interes Spółki, wniesienia:
        a. pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację,
        b. sprzeciwu wobec przetwarzania jej danych, gdy Administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

4. W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź musi nastąpić w terminie 30 dni od daty jego otrzymania. Odpowiedź może być udzielona na piśmie lub w innej formie wskazanej przez wnioskodawcę.

5. Osoba, której dane dotyczą, może się zwracać z wnioskiem o udzielenie informacji, nie częściej niż raz na 6 miesięcy. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, Spółka pobierze opłatę w rozsądnej wysokości, wynikającej z kosztów administracyjnych.

6. W sytuacji wniesienia przez osobę sprzeciwu wobec przetwarzania jej danych, informacja o wniesieniu sprzeciwu przekazywana jest do Administratora lub IOD (jeśli został ustanowiony). Dalsze przetwarzanie kwestionowanych danych jest niedopuszczalne. Administrator danych może jednak pozostawić w zbiorze imię lub imiona i nazwisko osoby oraz numer PESEL lub adres wyłącznie w celu uniknięcia ponownego wykorzystania danych tej osoby w celach objętych sprzeciwem.

7. Osoba, której dane dotyczą, ma prawo żądania od Spółki niezwłocznego usunięcia dotyczących jej danych osobowych, a Spółka ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeśli spełnione są przesłanki wystosowania takiego żądania. Jeżeli w toku działalności Spółka upubliczni takie dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje. Nie dotyczy to przekazania danych w celu wykonania przepisów prawa lub dochodzenia roszczeń.

8. Realizacja prawa do przenoszenia danych może mieć miejsce jedynie w przypadku przetwarzania danych na podstawie zgody lub w celu wykonania umowy. W takim przypadku osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu dane osobowe jej dotyczące, które dostarczyła Spółka.

§ 10. ZADANIA OSÓB ODPOWIEDZIALNYCH ZA OCHRONĘ DANYCH

1. Za bezpieczeństwo danych odpowiadają:
   1) Administrator Danych Osobowych,
   2) Inspektor Ochrony Danych;
   3) Administrator Systemu Informatycznego;
   4) pracownicy upoważnieni do przetwarzania danych osobowych.

2. Zadania IOD obejmują:
   1) uczestniczenie w tworzeniu, wdrażaniu i interpretowaniu dokumentacji ochrony danych osobowych standardów, zaleceń oraz procedur, dotyczących przetwarzania danych osobowych,
   2) koordynowanie działań w zakresie ochrony danych osobowych,
   3) monitorowanie przestrzegania przepisów prawa w zakresie danych osobowych, a także Polityki i Instrukcji,
   4) informowanie Administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów prawa,
   5) ścisłą współpracę z ASI w zakresie ustalenia zasad i nadzoru nad poprawnością przetwarzania danych osobowych w systemach informatycznych,
   6) zapoznanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami o ochronie danych osobowych poprzez przeprowadzenie szkoleń,
   7) prowadzenie Rejestru Czynności Przetwarzania,
   8) opiniowanie umów dotyczących powierzenia podmiotom trzecim przetwarzania danych osobowych,
   9) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń lub podejrzenia naruszenia zabezpieczeń,
   10) uczestnictwo w ocenie skutków dla ochrony danych osobowych,
   11) kontakt z organem nadzoru,
   12) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO.

3. Zadania ASI obejmują:
   1) rejestrowanie i wyrejestrowywanie użytkowników systemu,
   2) dokonywanie zmiany uprawnień użytkowników systemu,
   3) przestrzeganie opracowanych dla systemu procedur bezpieczeństwa,
   4) utrzymanie systemu informatycznego w sprawności technicznej,
   5) przeciwdziałanie dostępowi osób nieupoważnionych do systemu informatycznego, w którym przetwarzane są dane osobowe,
   6) konfigurowanie urządzeń i oprogramowania służących do przetwarzania danych osobowych, według zapotrzebowania,
   7) aktualizowanie i konfigurowanie oprogramowania antywirusowego,
   8) reagowanie na naruszenia bezpieczeństwa i usuwanie ich skutków,

9) nadzorowanie właściwego użytkowania oraz serwisowania urządzeń i oprogramowania,
10) prowadzenie dziennika pracy systemu, który zawiera opisy wszelkich zdarzeń istotnych dla działania systemu informatycznego, w szczególności w przypadku awarii – opis awarii, przyczyna awarii, szkody wynikłe na skutek awarii, sposób usunięcia awarii, opis systemu po awarii, wnioski,
11) w przypadku konserwacji systemu – opis podjętych działań, wnioski,
12) wykonywanie kopii bezpieczeństwa informatycznych baz, w których przetwarzane są dane osobowe oraz systemów informatycznych,
13) prowadzenie dokumentacji technicznej systemów,
14) informowanie ADO lub IOD o wszelkich zdarzeniach związanych lub mogących mieć wpływ na bezpieczeństwo systemu teleinformatycznego.

4. Pracownicy, niezależnie od stosunku prawnego regulującego podstawę ich zatrudnienia, zobowiązani są do:
   1) zachowania w tajemnicy danych osobowych, do których mają dostęp, a także sposobów zabezpieczenia tych danych, zarówno w trakcie jak i po ustaniu tego stosunku,
   2) przestrzegania przepisów wewnętrznych obowiązujących w Spółce wiążących się z ochroną danych osobowych, w tym Polityki i Instrukcji,
   3) zgłaszania zauważonych incydentów bezpieczeństwa związanych z ochroną danych osobowych.

§ 11. ODBIORCY DANYCH

1. Za odbiorców danych w rozumieniu niniejszej Polityki należy uznać wszystkie podmioty, które otrzymują od nas dane osobowe, w tym w szczególności:
    1) podmioty przetwarzające - podmioty, które nie decydują samodzielnie o celach i środkach przetwarzania danych, ale wykonują pewne czynności przetwarzania danych na zlecenie i w wykonaniu celów Spółki, w oparciu o art. 28 RODO,
    2) podmioty trzecie – inni odbiorcy danych, w tym inni administratorzy danych, którzy otrzymują dane osobowe w oparciu o przepisy art. 6 ust. 1 RODO.

2. Powierzenie przetwarzania danych osobowych podmiotowi przetwarzającemu wymaga zawarcia umowy w formie pisemnej, określającej w szczególności przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora zgodnie z art. 28 RODO.

3. Spółka może korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi przewidziane przepisami prawa i chroniło prawa osób, których dane dotyczą. Do osoby odpowiedzialnej za zawarcie umowy z takim podmiotem należy dołożenie starań, celem ustalenia, że podmiot ten spełnia powyższe warunki.

4. Dane osobowe przetwarzane przez Spółkę nie mogą być udostępniane podmiotom trzecim, chyba że istnieje podstawa prawna dla udostepnienia tych danych osobowych, a w szczególności osoba, której dane dotyczą wyraziła zgodę na udostępnienie jej danych podmiotowi trzeciemu lub istnieje przepis prawa nakazujący takie udostępnienie.

5. Możliwość przekazywania lub udostępniania danych osobowych podmiotom spoza Unii Europejskiej jest szczególnie ograniczona. W każdym przypadku takie przekazanie wymaga przeanalizowania jego dopuszczalności na gruncie przepisów art. 44-50 RODO.

6. Jest niezmiernie ważne, by każda osoba przetwarzająca dane osobowe w Spółce przekazywała dane odbiorcom danym jedynie wówczas, gdy takie przekazanie spełnia wymogi niniejszej Polityki. Sam proces przekazywania powinien być każdorazowo uwzględniony w Rejestrze Czynności Przetwarzania. Jeśli więc potrzebujesz przekazać dane podmiotowi przetwarzającemu lub podmiotowi trzeciemu, a taka możliwość nie wynika z Rejestru Czynności Przetwarzania, przed przekazaniem danych osobowych skonsultuj to z bezpośrednim przełożonym lub Inspektorem Ochrony Danych.

§ 12. POSTĘPOWANIE Z INCYDENTAMI

1. Incydentem jest każde naruszenie zasad ochrony danych osobowych, w szczególności:
   1) nieuprawniony dostęp lub próba dostępu do danych osobowych,
   2) udostępnianie danych osobom nieupoważnionym,
   3) przetwarzanie danych przez osoby nieupoważnione,
   4) utrata danych zapisanych na kopiach zapasowych,
   5) naruszenie poufności, integralności lub dostępności danych.

2. Każdy pracownik Spółki, niezależnie od stosunku prawnego regulującego podstawę jego zatrudnienia, w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować o tym bezpośredniego przełożonego lub Inspektora Ochrony Danych, w terminie nie dłuższym niż 24 h od wystąpienia incydentu, a w przypadku jeśli incydent wystąpi w przeddzień dnia wolnego od pracy, jeszcze w tym samym dniu.

3. W przypadku stwierdzenia incydentu (naruszenia), Inspektor Ochrony Danych prowadzi postępowanie wyjaśniające, w toku którego:
   1) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
   2) zabezpiecza ewentualne dowody,
   3) ustala osoby odpowiedzialne za naruszenie,
   4) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
   5) inicjuje działania dyscyplinarne,
   6) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
   7) dokumentuje prowadzone postępowania,
   8) sporządza raport z incydentu.

4. Tryb postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego określa Instrukcja.

5. Po otrzymaniu informacji o wystąpieniu incydentu Inspektor Ochrony Danych ocenia, czy incydent ten skutkował ryzykiem naruszenia praw lub wolności osób fizycznych i raportuje swoje wnioski do Zarządu. W przypadku stwierdzenia prawdopodobieństwa takiego ryzyka, w terminie nie dłuższym niż 72 h od wystąpienia incydentu, Spółka zgłasza to naruszenie Prezesowi Urzędu Ochrony Danych Osobowych (lub jego odpowiednikowi, tj. Generalnemu Inspektorowi Ochrony Danych Osobowych).

6. Administrator prowadzi rejestr incydentów, zawierający w szczególności opis okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

§ 13. ODPOWIEDZIALNOŚĆ

1. Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami określonymi w art. 83 RODO, Ustawy oraz w art. 266 - 269 Kodeksu karnego.

2. W związku z powyższym wszelkie incydenty związane z naruszeniem zasad ochrony danych osobowych mogą skutkować zarówno odpowiedzialnością bezpośrednią osób, które do incydentu dopuściły, jak i odpowiedzialnością finansową Spółki.

3. Niezależnie od odpowiedzialności przewidzianej w przepisach, o których mowa w ust. 1, naruszenie zasad ochrony danych osobowych obowiązujących w Spółce, może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną lub rozwiązaniem umowy cywilnoprawnej.

ZAŁĄCZNIK NR 1. Rejestr Czynności Przetwarzania

[EXCEL]

ZAŁĄCZNIK NR 2. Wytyczne dotyczące oceny skutków dla ochrony danych

☐ Zapewniono systematyczny opis operacji przetwarzania (art. 35 ust. 7 lit. a RODO):
- ☐ uwzględniono charakter, zakres, kontekst i cele przetwarzania (motyw 90);
- ☐ w rejestrze zamieszczono dane osobowe, informacje o odbiorcach i okresie przechowywania danych osobowych;
- ☐ przedstawiono funkcjonalny opis operacji przetwarzania;
- ☐ zidentyfikowano zasoby, z którymi styczność mają dane osobowe (sprzęt komputerowy, oprogramowanie, sieci, osoby, opracowania lub kanały transmisji opracowań);
- ☐ uwzględniono przestrzeganie zatwierdzonych kodeksów postępowania (art. 35 ust. 8);

☐ Oceniono niezbędność oraz proporcjonalność (art. 35 ust. 7 lit. b) RODO):
- ☐ wskazano środki, których podjęcie jest planowane w celu zapewnienia przestrzegania rozporządzenia (art. 35 ust. 7 lit. d) i motyw 90), uwzględniając:
  - ☐ środki przyczyniające się do proporcjonalności i niezbędności przetwarzania, z uwzględnieniem następujących aspektów:
    - ☐ konkretne, wyraźne i prawnie uzasadnione cele (art. 5 ust. 1 lit. b));
    - ☐ zgodność przetwarzania z prawem (art. 6);
    - ☐ dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (art. 5 ust. 1 lit. c));
    - ☐ ograniczony czas przechowywania (art. 5 ust. 1 lit. e));
  - ☐ środki przyczyniające się do zachowania praw osób, których dane dotyczą:
    - ☐ poinformowanie osoby, której dane dotyczą (art. 12, 13 i 14);
    - ☐ prawo dostępu i prawo do przenoszenia danych (art. 15 i 20);
    - ☐ prawo do sprostowania i do usunięcia danych (art. 16, 17 i 19);
    - ☐ prawo do sprzeciwu i prawo do ograniczenia przetwarzania (art. 18, 19 i 21);
    - ☐ relacje z podmiotem przetwarzającym (art. 28);
    - ☐ zabezpieczenia przy międzynarodowym przekazywaniu danych (rozdział V);
    - ☐ uprzednie konsultacje (art. 36);

☐ Przeprowadzono działania w zakresie zarządzania ryzykiem naruszenia praw i wolności osób, których dane dotyczą (art. 35 ust. 7 lit. c) RODO):
- ☐ uwzględniono źródło, charakter, specyfikę i powagę ryzyka (por. motyw 84), czy konkretniej, w przypadku każdego rodzaju ryzyka (bezprawnego dostępu, niepożądanej zmiany i zniknięcia danych), z punktu widzenia osób, których dane dotyczą:
  - ☐ uwzględniono źródła ryzyka (motyw 90);
  - ☐ zidentyfikowano możliwe skutki dla praw i wolności osób, których dane dotyczą, w przypadku zdarzeń takich jak bezprawny dostęp, niepożądane zmiany i zniknięcie danych;
  - ☐ zidentyfikowano zagrożenia, które mogłyby doprowadzić do bezprawnego dostępu, niepożądanych zmian i zniknięcia danych;
  - ☐ oszacowano prawdopodobieństwo i powagę (motyw 90);
- ☐ określono środki, których podjęcie jest planowane w celu zaradzenia ryzyku (art. 35 ust. 7 lit. d) i motyw 90);

☐ Zaangażowano zainteresowane strony:
- ☐ skonsultowano się z inspektorem ochrony danych w celu uzyskania zalecenia (art. 35 ust. 2);
- ☐ w stosownych przypadkach zasięgnięto opinii osób, których dane dotyczą, lub ich przedstawicieli (art. 35 ust. 9).

ZAŁĄCZNIK NR 3. Wzór upoważnienia

Upoważnienie do przetwarzania danych

UPOWAŻNIENIE Nr .....

Działając w imieniu **W & W Nieruchomości A. Wójcik, J. Wójcik Spółka Jawna** z siedzibą w Gliwicach, ul. Kozielska 490, 44-164 Gliwice, wpisanej do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem KRS: 0000426110, posiadającej numer NIP: 9691522489 oraz REGON: 240913051 (dalej: **Spółka**) upoważniam:

Pana/Panią .....

do przetwarzania danych osobowych, których Spółka jest administratorem w następującym

zakresie .....

w celu .....

.....,

Upoważnienie wydano w dniu .....

Upoważnienie traci ważność z dniem rozwiązania umowy będącej podstawą zatrudnienia w Spółce lub odwołaniem upoważnienia.

Nr identyfikatora .....

/jeżeli dane przetwarzane są w systemie informatycznym/

.....

Data i podpis

Pouczenie

Osoba, która została upoważniona oświadcza, iż zapoznała się z dokumentacją wewnętrzną dotyczącą ochrony danych osobowych obowiązującą w Spółce i zobowiązuje się do przestrzegania jej postanowień, w szczególności obowiązana jest zachować w tajemnicy wobec osób nieuprawnionych przetwarzane dane osobowe oraz sposób ich zabezpieczenia.

Powyższe przyjmuję do wiadomości i wykonania:

.....

Data i podpis

ZAŁĄCZNIK NR 4. Rejestr upoważnionych

Lp.	Imię nazwisko	Zakres przydzielonych uprawnień	Data przyznania uprawnień	Data ustania uprawnień
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				