



drewplast

POLITYKA OCHRONY DANYCH OSOBOWYCH

Drewplast sp. z o.o.

Grabowno Wielkie 5E, 56-416 Twardogóra

Data wprowadzenia:

11/05/2024

SPIS TREŚCI

A. INFORMACJE OGÓLNE

1. Cel Polityki ochrony danych osobowych
2. Terminologia
3. Zakres informacji objętych Polityką ochrony danych osobowych oraz zakres zastosowania

B. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

1. Struktura organizacji ochrony danych osobowych
 - 1.1. Administrator Danych
 - 1.2. Osoby upoważnione do przetwarzania danych osobowych

C. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. Ogólne zasady przetwarzania danych osobowych
2. Zakres przetwarzanych danych osobowych
3. Dopuszczenie osób do przetwarzania danych osobowych
4. Powierzenie przetwarzania danych osobowych
5. Udostępnienie danych osobowych
6. Przekazywanie danych osobowych do państw trzecich
7. Współadministrowanie danymi osobowymi
8. Podejście oparte na ryzyku
9. Ocena ryzyka dla procesów lub sposobów organizacji przetwarzania danych osobowych
10. Ochrona danych osobowych w fazie projektowania oraz domyślna ochrona danych osobowych
11. Ocena skutków dla ochrony danych osobowych (*data protection impact assessment*)
12. Test równowagi prawnie uzasadnionego interesu Administratora Danych (*balancing test*)
13. Naruszenia ochrony danych osobowych
14. Realizacja praw osób, których dane dotyczą
15. Ogólne zasady bezpieczeństwa ochrony danych osobowych
16. Przeglądy i aktualizacja Polityki ochrony danych osobowych
17. Załączniki

A. INFORMACJE OGÓLNE

1. CEL POLITYKI OCHRONY DANYCH OSOBOWYCH

Polityka ochrony danych osobowych została opracowana i wdrożona w strukturze Administratora Danych w celu zapewnienia zgodności przetwarzania danych osobowych z wymogami obowiązujących w tym zakresie polskich i europejskich aktów prawnych, w szczególności:

1. Rozporządzenia 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),
2. Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000 ze zm.).

Polityka ochrony danych osobowych ma zastosowanie do wszystkich pracowników Administratora Danych, którzy w zakresie swoich obowiązków służbowych przetwarzają dane osobowe, jak również innych osób, które z upoważnienia Administratora Danych uzyskały dostęp do danych osobowych. Każda z tych osób została zapoznana z najważniejszymi procedurami bezpieczeństwa danych opisanymi w Polityce ochrony danych osobowych i zobowiązana do ich przestrzegania w zakresie wynikającym z przydzielonych zadań. Osoby, o których mowa złożyły oświadczenie o zapoznaniu się z procedurami bezpieczeństwa danych oraz zobowiązały się do ich stosowania.

Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów Polityki ochrony danych osobowych, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

2. TERMINOLOGIA

1. **Administrator Danych** – Drewplast sp. z o.o., Grabowno Wielkie 5E, 56-416 Twardogóra, w imieniu którego działa prezes zarządu, uprawniony do reprezentowania spółki,
2. **dane osobowe** – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”), gdzie poprzez możliwą do zidentyfikowania osobę fizyczną rozumie się osobę, 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,
3. **DPIA** – ocena skutków dla ochrony danych osobowych (*data protection impact assessment*),
4. **organ nadzorczy** – niezależny organ publiczny powołany w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii, powołany w każdym państwie członkowskim Unii, którego podstawowym zadaniem jest monitorowanie stosowania RODO,
5. **państwo trzecie** – państwo nienależące do Europejskiego Obszaru Gospodarczego.
6. **podmiot przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych,
7. **Polityka** – niniejsza Polityka ochrony danych osobowych,
8. **pracownik** – osoba współpracująca z Administratorem Danych na podstawie umowy o pracę lub umowy cywilnoprawnej,
9. **przetwarzanie** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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,
10. **RODO** – Rozporządzenie 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),
11. **Unia** – Unia Europejska,
12. **Ustawa** – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000 ze zm.).

3. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ OCHRONY DANYCH OSOBOWYCH ORAZ ZAKRES ZASTOSOWANIA

Polityka ochrony danych osobowych opisuje zasady i procedury przetwarzania danych osobowych. Jest to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Administratora Danych. Polityka ochrony danych osobowych odnosi się całościowo do problemu zabezpieczenia danych osobowych, tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych.

Politykę ochrony danych osobowych stosuje się do wszelkich czynności, stanowiących w myśl RODO, przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosowane są zasady ujęte w Polityce.

Rygorowi Polityki podlegają także dane powierzone Administratorowi Danych do przetwarzania na podstawie umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego oraz dane osobowe, które zostały Administratorowi Danych udostępnione.

B. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

1. STRUKTURA ORGANIZACJI OCHRONY DANYCH OSOBOWYCH

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami RODO, Ustawy, Polityki oraz procedur wewnętrznych z zakresu ochrony danych osobowych wdrożonych w strukturze Administratora Danych, odpowiadają:

1. Administrator Danych,
2. Osoby upoważnione do przetwarzania danych osobowych.

1.1. ADMINISTRATOR DANYCH

1. Administrator Danych jest odpowiedzialny za:
 - 2.1. zapewnienie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia i wykazania przetwarzania danych osobowych zgodnie z zasadami przetwarzania danych osobowych określonymi w RODO,
 - 2.2. opracowywanie i aktualizacja Polityki, wdrożenie procedur ochrony danych osobowych,
 - 2.3. zapewnienie środków umożliwiających prawidłową realizację praw osób, których dane dotyczą, oraz pełnienie funkcji punktu kontaktowego dla tychże osób we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych,
 - 2.4. prowadzenie rejestru czynności przetwarzania danych osobowych,
 - 2.5. prowadzenie rejestru kategorii czynności przetwarzania dokonywanych w imieniu innego administratora,
 - 2.6. współpracę z organem nadzorczym w ramach wykonywania przez niego swoich zadań,
 - 2.7. wdrożenie odpowiednich środków organizacyjnych i technicznych, aby zapewnić stopień bezpieczeństwa odpowiadający istniejącemu ryzyku naruszenia praw lub wolności osób, których dane dotyczą,
 - 2.8. zgłaszanie naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu, a w przypadku, gdy zajdą ku temu odpowiednie przesłanki, również osobie, której dane dotyczą,
 - 2.9. dokumentowanie wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych (rejestr naruszeń),
 - 2.10. zapewnienie odpowiednich środków w celu dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w sytuacji, jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym, jeżeli zajdą ku temu odpowiednie przesłanki, konsultacje z organem nadzorczym,

- 2.11. nadawanie upoważnień do przetwarzania danych osobowych, ich administrowanie oraz kontrola, w tym prowadzenie ewidencji osób upoważnionych,
- 2.12. zapewnienie legalności przekazywania danych osobowych do podmiotów trzecich,
- 2.13. szkolenia dla pracowników Administratora Danych uczestniczących w operacjach przetwarzania danych oraz inne działania zwiększające świadomość pracowników w zakresie obowiązków wynikających z RODO lub przyjętych procedur,
- 2.14. opracowywanie unikalnych treści klauzul informacyjnych, klauzul zgód na przetwarzanie danych osobowych, umów powierzenia przetwarzania danych osobowych oraz innych klauzul / postanowień związanych z przetwarzaniem danych osobowych (np. postanowień w zakresie współadministrowania),
- 2.15. kontrola podmiotów przetwarzających,
- 2.16. kontrola systemów informatycznych, w tym:
 - 2.16.1. opracowywanie oraz aktualizacja **Załącznika nr 11** do Polityki, który stanowi ogólny opis technicznych środków bezpieczeństwa wdrożonych w strukturze Administratora Danych,
 - 2.16.2. nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
 - 2.16.3. podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
 - 2.16.4. identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych,
 - 2.16.5. sprawowanie nadzoru nad kopiami zapasowymi,
 - 2.16.6. inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych.

1.2. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych, zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO, Ustawy oraz postanowieniami Polityki.
2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia. Stosowny zapis o przyjęciu zobowiązania do zachowania w tajemnicy przetwarzanych danych osobowych zawiera upoważnienie, którego wzór znajduje się w **Załączniku nr 2** do Polityki.

3. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów Ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (tekst jedn. Dz.U. z 2018 r., poz. 108 ze zm.), bądź rozwiązania stosunku cywilnoprawnego.

C. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych w strukturze Administratora Danych odbywa się zgodnie z ogólnymi zasadami przetwarzania danych osobowych określonymi w art. 5 RODO. Oznacza to, że dane osobowe przetwarzają się:
 - 1.1 zgodnie z prawem, w oparciu o co najmniej jedną przesłankę legalności przetwarzania danych osobowych wskazaną w art. 6 lub 9 RODO (*zasada legalności*),
 - 1.2 w sposób rzetelny przy uwzględnieniu interesów i rozsądnych oczekiwań osób, których dane dotyczą (*zasada rzetelności*),
 - 1.3 w sposób przejrzysty dla osób, których dane dotyczą (*zasada przejrzystości*),
 - 1.4 w konkretnych, wyraźnych i prawnie uzasadnionych celach (*zasada ograniczenia celu*),
 - 1.5 w zakresie adekwatnym, stosownym oraz niezbędnym dla celów, w których są przetwarzane (*zasada minimalizacji danych*),
 - 1.6 przy uwzględnieniu ich prawidłowości i ewentualnego uaktualniania (*zasada prawidłowości*),
 - 1.7 przez okres nie dłuższy, niż jest to niezbędne dla celów, w których są przetwarzane (*zasada ograniczenia przechowywania*),
 - 1.8 w sposób zapewniający odpowiednie bezpieczeństwo (*integralność i poufność*).
2. Administrator Danych gwarantuje, że określone decyzje odnoszące się do procesów przetwarzania danych osobowych zostały przeanalizowane z punktu widzenia zgodności z ogólnymi zasadami przetwarzania danych, a przede wszystkim, że są z nimi zgodne.

2. ZAKRES PRZETWARZANYCH DANYCH OSOBOWYCH

1. Polityka ma zastosowanie w stosunku do wszystkich danych osobowych przetwarzanych przez Administratora Danych, niezależnie od formy ich przetwarzania (elektroniczna lub papierowa) oraz tego, czy są to dane przetwarzane w zbiorach danych, w zestawach czy stanowią one pojedyncze informacje osobowe.
2. Administrator Danych prowadzi:
 - 2.1. rejestr czynności przetwarzania danych osobowych, których jest administratorem,
 - 2.2. rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratorów, którzy powierzyli mu przetwarzanie danych, o ile takie okoliczności mają miejsce.
3. Rejestr, o którym mowa w pkt 2.1. zawiera co najmniej następujące informacje:
 - 3.1. nazwę oraz dane kontaktowe Administratora Danych oraz wszelkich współadministratorów,
 - 3.2. gdy ma to zastosowanie imię, nazwisko lub nazwę oraz dane kontaktowe swojego przedstawiciela,
 - 3.3. cele przetwarzania,
 - 3.4. opis kategorii osób, których dane dotyczą,
 - 3.5. opis kategorii danych osobowych,
 - 3.6. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
 - 3.7. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,
 - 3.8. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
 - 3.9. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
4. Rejestr, o którym mowa w pkt 2.2. zawiera co najmniej następujące informacje:
 - 4.1. nazwę oraz dane kontaktowe Administratora Danych,
 - 4.2. imię i nazwisko lub nazwę oraz dane kontaktowe każdego administratora, w imieniu którego działa Administrator Danych,
 - 4.3. gdy ma to zastosowanie, imię, nazwisko lub nazwę oraz dane kontaktowe przedstawiciela każdego administratora, w imieniu którego działa Administrator Danych,
 - 4.4. gdy ma to zastosowanie, imię i nazwisko oraz dane kontaktowe IOD każdego administratora, w imieniu którego działa Administrator Danych,
 - 4.5. kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,
 - 4.6. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w

przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,

- 4.7. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
5. Administrator Danych prowadzi rejestry, o których mowa w pkt 2 w formie pisemnej, w tym elektronicznej.
6. W przypadku zgłoszenia przez organ nadzorczy żądania w tym zakresie, Administrator Danych udostępnia mu prowadzone przez siebie rejestry.

3. DOPUSZCZENIE OSÓB DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych realizując Politykę, w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie osobom, które uzyskały uprzednie, stosowne upoważnienie do przetwarzania danych osobowych.
2. Upoważnienie do przetwarzania danych osobowych nadawane jest po przeprowadzeniu szkolenia lub zaznajomieniu w innej formie, osoby upoważnianej z zasadami ochrony danych osobowych obowiązującymi w strukturze Administratora Danych.
3. Upoważnienie do przetwarzania danych osobowych, nadawane jest indywidualnie, z wyraźnym wskazaniem, jakie zbiory danych obejmuje swoim zakresem.
4. Administrator Danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, która zawiera co najmniej takie informacje jak:
 - 4.1. imię i nazwisko osoby upoważnionej,
 - 4.2. zakres upoważnienia,
 - 4.3. data nadania upoważnienia,
 - 4.4. data ustania upoważnienia.
5. Ewidencja osób upoważnionych do przetwarzania danych osobowych prowadzona jest w formie pisemnej, w tym elektronicznej
6. Szczegółowa Procedura szkoleń oraz nadawania upoważnień do przetwarzania danych osobowych stanowi **Załącznik nr 2** do Polityki.

4. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przetwarzane poza własnymi strukturami organizacyjnymi. Może się to odbywać wyłącznie na drodze powierzenia danych, w określonym celu i zakresie, podmiotowi przetwarzającemu na mocy umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego.
2. Podstawowym warunkiem dopuszczalności powierzenia przetwarzania danych w imieniu administratora jest poddanie planowanego outsourcingu analizie, która powinna zapewnić, że wybór podmiotu przetwarzającego został uzależniony od zapewnienia wystarczających gwarancji ochrony danych.
3. Zawierana przez Administratora Danych umowa powierzenia przetwarzania danych osobowych musi być zgodna z postanowieniami art. 28 RODO, tj. w szczególności określać:
 - 3.1. przedmiot powierzenia,
 - 3.2. czas trwania powierzenia,
 - 3.3. charakter i cel przetwarzania,
 - 3.4. rodzaj powierzanych danych osobowych,
 - 3.5. kategorie osób, których dane dotyczą,
 - 3.6. warunki podpowierzenia przetwarzania danych
 - 3.7. obowiązki i prawa Administratora Danych,
 - 3.8. obowiązki podmiotu przetwarzającego.
4. Umowa powierzenia może zostać zawarta w formie pisemnej, w tym w elektronicznej.
5. W przypadku, gdy elementy powierzenia przetwarzania danych wskazane w pkt 3 znajdują się już w zawartej z danym podmiotem umowie, nie ma konieczności sporządzania dodatkowej umowy powierzenia przetwarzania danych osobowych.
6. Każdorazowe dokonanie powierzenia danych osobowych musi zostać obligatoryjnie odnotowane w rejestrze czynności przetwarzania danych osobowych.
7. Administrator Danych ma prawo kontroli podmiotów przetwarzających, którym powierzył przetwarzanie danych osobowych. Procedura kontroli podmiotów przetwarzających stanowi **Załącznik nr 9** do Polityki.
8. Administrator Danych w zakresie prowadzonej przez siebie działalności może przetwarzać również dane osobowe powierzone przez podmioty, na rzecz których świadczy usługi. Przyjęcie danych w powierzenie przez Administratora Danych musi zostać obligatoryjnie odnotowane w rejestrze kategorii czynności przetwarzania danych osobowych.

5. UDOSTĘPNIENIE DANYCH OSOBOWYCH

1. Administrator Danych realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przekazywane innym administratorom w formie udostępnienia danych.
2. Udostępnienie danych osobowych może nastąpić tylko w oparciu o co najmniej jedną przesłankę spośród wskazanych w art. 6 RODO i / lub art. 9 RODO.
3. Podmioty lub kategorie podmiotów, którym udostępnia się dane osobowe muszą zostać obligatoryjnie wskazane w rejestrze czynności przetwarzania danych osobowych.

6. PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH

1. Przekazywanie danych, których administratorem jest Administrator Danych do państw trzecich i organizacji międzynarodowych, może się odbywać wyłącznie po spełnieniu warunków przewidzianych w Rozdziale V RODO.
2. Przekazywanie danych do państw trzecich może mieć formę zarówno powierzenia przetwarzania danych osobowych oraz udostępnienia danych osobowych, co oznacza, że w zależności od rodzaju przekazania, należy wziąć również pod uwagę postanowienia podrozdziałów 4 i 5 Polityki.
3. Przekazanie danych osobowych, których administratorem jest Administrator Danych do państwa trzeciego może nastąpić w sytuacji, jeżeli Komisja Europejska wydała decyzję, że dane państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.
4. W przypadkach braku decyzji Komisji Europejskiej, o której mowa w pkt 3, dokonanie przekazania danych osobowych do państwa trzeciego jest możliwe, gdy Administrator Danych samodzielnie zapewni odpowiednie zabezpieczenia i pod warunkiem, że będą obowiązywały egzekwowalne prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej. Odpowiednie zabezpieczenia Administrator Danych może zapewnić za pomocą:
 - 4.1. wiążących reguł korporacyjnych zatwierdzonych przez organ nadzorczy, mających zastosowanie do każdego z członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą,
 - 4.2. standardowych klauzul ochrony danych przyjętych lub zatwierdzonych przez Komisję Europejską,
 - 4.3. standardowych klauzul ochrony danych przyjętych przez organ nadzorczy i zatwierdzonych przez Komisję Europejską,
 - 4.4. zatwierzonego kodeksu postępowania wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą, lub
 - 4.5. zatwierzonego mechanizmu certyfikacji wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą.
5. Z zastrzeżeniem zezwolenia właściwego organu nadzorczego odpowiednie zabezpieczenia, o których mowa w pkt 4 Administrator Danych może zapewnić w szczególności za pomocą klauzul umownych między Administratorem Danych lub podmiotem przetwarzającym a Administratorem Danych, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim lub organizacji międzynarodowej.
6. W szczególnych przypadkach, dopuszcza się przekazanie danych osobowych przez Administratora Danych do państwa trzeciego pomimo braku decyzji Komisji Europejskiej, o której mowa w pkt 3 oraz zapewnienia odpowiednich zabezpieczeń, o których mowa w pkt 4 i 5. Do tych szczególnych przypadków zalicza się przekazanie danych pod warunkiem, że:
 - 6.1. osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którymi może się dla niej wiązać proponowane przekazanie, wyrazi na nie wyraźną zgodę,

- 6.2. przekazanie jest niezbędne do wykonania umowy zawartej z osobą, której dane dotyczą,
- 6.3. przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą,
- 6.4. przekazanie jest niezbędne ze względu na ważne względy interesu publicznego,
- 6.5. przekazanie jest niezbędne ze względu na posiadane roszczenia,
- 6.6. przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą lub
- 6.7. przekazanie nastąpi z publicznego rejestru.

7. WSPÓŁADMINISTROWANIE DANYMI OSOBOWYMI

1. Administrator Danych w zakresie przetwarzanych przez siebie danych osobowych dopuszcza możliwość przyjęcia modelu współadministrowania danymi osobowymi zgodnie z art. 26 RODO.
2. Współadministrowanie danymi może zachodzić wówczas, jeżeli Administrator Danych oraz co najmniej jeden inny podmiot, wspólnie ustalają cele i sposoby przetwarzania danych osobowych. Oznacza to, że w danym procesie przetwarzania danych osobowych muszą zostać spełnione równocześnie trzy warunki, tj. Administrator Danych oraz co najmniej jeden inny podmiot muszą:
 - 2.1. być administratorami w rozumieniu art. 4 pkt 7 RODO,
 - 2.2. muszą wspólnie ustalić cele przetwarzania danych,
 - 2.3. muszą wspólnie ustalić sposoby (techniczne i organizacyjne) przetwarzania danych osobowych.
3. W przypadku spełnienia warunków, o których mowa w pkt 2 Administrator Danych oraz co najmniej jeden inny podmiot stają się współadministratorami danych w zakresie danego procesu przetwarzania danych osobowych.
4. W przypadku przyjęcia modelu współadministrowania danymi, współadministratorzy danych w drodze wspólnych uzgodnień, w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.
5. Administrator Danych dokonuje oceny, czy dany proces przetwarzania spełnia warunki współadministrowania danymi.
6. W przypadku, kiedy wynik oceny, o której mowa w pkt 5 wskazuje na współadministrowanie danymi osobowymi, Administrator Danych, przy współudziale pozostałych współadministratorów, opracowuje wspólne uzgodnienia, o których mowa w pkt 4.

8. PODEJŚCIE OPARTE NA RYZYKU

1. W zakresie stosowanych rozwiązań odnoszących się do przetwarzania danych osobowych, a w szczególności w zakresie zabezpieczeń, Administrator Danych stosuje zasadę podejścia opartego na ryzyku (*risk-based approach*).
2. Administrator Danych uzależnia sposób realizacji nałożonych na niego obowiązków od charakteru, zakresu, kontekstu i celów przetwarzania danych oraz od ryzyka naruszenia praw i wolności osób, których dane dotyczą, a także ryzyka naruszenia interesów Administratora Danych.
3. Realizując zasadę podejścia opartego na ryzyku, Administrator Danych:
 - 3.1. respektuje to, że RODO szczególnie nacisk kładzie na ochronę praw i wolności osób, których dane osobowe są przetwarzane,
 - 3.2. dostosowuje środki ochrony danych osobowych do skali ryzyka naruszenia praw i wolności osób fizycznych, których dane dotyczą,
 - 3.3. koncentruje się na poszukiwaniu i wdrażaniu środków redukujących prawdopodobieństwo i skutki wystąpienia najbardziej dotkliwych zagrożeń,
 - 3.4. dokonuje monitorowania i regularnych przeglądów procesów i sposobów organizacji przetwarzania danych osobowych.
4. Stosowana przez Administratora Danych zasada podejścia opartego na ryzyku jest procesem ciągłym, wymagającym stałej identyfikacji i szacowania poziomu ryzyka związanego z przetwarzaniem danych osobowych. W strukturze Administratora Danych następuje to, w szczególności poprzez:
 - 4.1. przeprowadzanie oceny ryzyka dla procesów lub sposobów organizacji przetwarzania danych osobowych (Podrozdział 9 Polityki),
 - 4.2. dokonywanie kwalifikacji procesów przetwarzania danych osobowych pod kątem konieczności poddania ich ocenie skutków dla ochrony danych osobowych (Podrozdział 11 Polityki),
 - 4.3. przeprowadzanie oceny skutków dla ochrony danych osobowych (Podrozdział 11 Polityki),
 - 4.4. stosowanie tzw. zasad *privacy by design* i *privacy by default* (Podrozdział 10 Polityki),
 - 4.5. przeprowadzanie testów równowagi prawnie uzasadnionego interesu Administratora Danych (Podrozdział 12 Polityki),
 - 4.6. stały monitoring otoczenia prawnego mającego wpływ na przetwarzanie danych osobowych przez Administratora Danych (monitoring zewnętrzny),
 - 4.7. stały monitoring realizacji wypracowanych założeń w zakresie ochrony danych osobowych w ramach struktury Administratora Danych (monitoring wewnętrzny).

9. OCENA RYZYKA DLA PROCESÓW LUB SPOSOBÓW ORGANIZACJI PRZETWARZANIA DANYCH OSOBOWYCH

1. Ocena ryzyka dla procesów lub sposobów organizacji przetwarzania danych osobowych przeprowadzana jest w sytuacjach, gdy istnieje uzasadnione podejrzenie, że dany proces lub sposób organizacji przetwarzania danych osobowych może nieść za sobą ryzyko naruszenia praw lub wolności osób, których dane dotyczą. W szczególności dotyczy to procesów lub sposobu organizacji przetwarzania danych osobowych, które wiążą się z zastosowaniem technologii, zarówno nowych jak i tych, które uległy znacznej zmianie w stosunku do ich pierwotnego charakteru lub zastosowania.
2. Procedura oceny ryzyka dla procesów lub sposobów organizacji przetwarzania danych osobowych stanowi **Załącznik nr 4A** do Polityki.

10. OCHRONA DANYCH OSOBOWYCH W FAZIE PROJEKTOWANIA ORAZ DOMYŚLNA OCHRONA DANYCH OSOBOWYCH

1. Administrator Danych wdraża odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych osobowych, nadania przetwarzaniu danych niezbędnych zabezpieczeń oraz zapewnieniu ochrony praw osób, których dane dotyczą.
2. Wdrażając odpowiednie środki techniczne i organizacyjne Administrator Danych uwzględnia:
 - 2.1. stan wiedzy technicznej,
 - 2.2. koszt wdrażania,
 - 2.3. charakter, zakres, kontekst i cele przetwarzania danych,
 - 2.4. ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania.
3. Administrator Danych wdraża takie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia określonego celu przetwarzania, biorąc pod uwagę: ilość zbieranych danych osobowych, ich zakres, okres ich przechowywania oraz ich dostępność dla innych osób.
4. W szczególności, stosowane środki techniczne i organizacyjne muszą zapewnić, by domyślnie dane osobowe nie były udostępniane nieokreślonej liczbie osób.
5. W pierwszej kolejności, Administrator Danych rozważa, czy cel jakiego ma służyć projektowane rozwiązanie jest możliwy do osiągnięcia bez konieczności przetwarzania danych osobowych. Jeśli tak, należy wybrać takie rozwiązanie.
6. Ogólny opis organizacyjnych i fizycznych środków bezpieczeństwa wdrożonych w strukturze Administratora Danych stanowi **Załącznik nr 10** do Polityki.
7. Ogólny opis technicznych środków bezpieczeństwa wdrożonych w strukturze Administratora Danych stanowi **Załącznik nr 11** do Polityki.

11. OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH (*DATA PROTECTION IMPACT ASSESSMENT*)

1. Administrator Danych dokonuje kwalifikacji procesów przetwarzania danych osobowych pod kątem konieczności poddania ich ocenie skutków dla ochrony danych osobowych.
2. Administrator Danych, w przypadkach uzasadnionych, dokonuje oceny skutków dla ochrony danych osobowych w celu opisanego przetwarzania danych osobowych oraz oceny jego konieczności i proporcjonalności, a także w celu wspomagania zarządzania ryzykiem naruszenia praw i wolności osób fizycznych wynikającym z przetwarzania ich danych osobowych.
3. Procedura oceny skutków dla ochrony danych osobowych (*data protection impact assessment*) stanowi **Załącznik nr 5** do Polityki.

12. TEST RÓWNOWAGI PRAWNIE UZASADNIONEGO INTERESU ADMINISTRATORA DANYCH (*BALANCING TEST*)

1. W przypadkach, kiedy Administrator Danych przetwarza lub planuje przetwarzać dane osobowe na podstawie art. 6 ust. 1 lit. f) RODO tj. do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora Danych lub przez stronę trzecią, jest on zobowiązany do przeprowadzenia tzw. testu równowagi (*balancing test*).
2. Prawnne uzasadnione interesy Administratora Danych lub strony trzeciej, mogą być podstawą przetwarzania danych wyłącznie wtedy, o ile w świetle rozsądnych oczekiwań osób, których dane dotyczą, opartych na ich powiązaniach z Administratorem Danych nadrzędne nie są interesy lub podstawowe prawa i wolności osoby, której dane dotyczą.
3. Procedura testu równowagi prawnie uzasadnionego interesu Administratora Danych stanowi [Załącznik nr 6](#) do Polityki.

13. NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Za bezpieczeństwo danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do pomieszczeń oraz systemów, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszenia ochrony danych osobowych, odpowiedzialny jest Administrator Danych.
2. Procedura postępowania z incydentami ochrony danych osobowych stanowi [Załącznik nr 3A](#) do Polityki.

14. REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

1. Administrator Danych uwzględni w zachodzących w jego strukturze procesach przetwarzania danych osobowych, procedury i zasady ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy przepisów RODO, w tym, w szczególności:
 - 1.1. prawo do wycofania wyrażonej zgody (art. 7 ust. 3 RODO),
 - 1.2. prawo dostępu przysługujące osobie, której dane dotyczą (art. 15 RODO),
 - 1.3. prawo do sprostowania danych (art. 16 RODO),
 - 1.4. prawo do usunięcia danych (w tym prawo do bycia zapomnianym) (art. 17 RODO),
 - 1.5. prawo do ograniczenia przetwarzania (art. 18 RODO),
 - 1.6. prawo do przenoszenia danych (art. 20 RODO),
 - 1.7. prawo sprzeciwu (art. 21 RODO),
 - 1.8. prawo do niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu (art. 22 RODO).
2. Procedura realizacji praw osób, których dane dotyczą stanowi **Załącznik nr 7** do Polityki.

15. OGÓLNE ZASADY BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

1. Dostęp do danych osobowych mogą mieć tylko pracownicy posiadający upoważnienie do ich przetwarzania.
2. Przebywanie osób nieuprawnionych do przetwarzania danych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania, chyba, że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
3. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem, w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
4. Pracownicy przechowujący dane osobowe zobowiązani są do zabezpieczenia materiałów zawierających dane osobowe w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym.
5. Niedopuszczalnym jest wnoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
6. Nikomu nie należy udostępniać indywidualnych haseł i identyfikatorów do systemów informatycznych.
7. Wysyłanie seryjnych wiadomości e-mail wymaga zastosowania opcji *kopia ukryta*.
8. Nie można udzielać informacji dotyczących danych osobowych innym podmiotom na podstawie prośby o takie dane skierowanej w formie zapytania telefonicznego.
9. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. *czystego biurka*, która oznacza niepozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację zasady odpowiedzialny jest na swym stanowisku każdy z pracowników. Nie należy pozostawiać danych osobowych w miejscach ogólnodostępnych takich jak np. biurka, blaty, parapety.
10. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe odbywać się musi w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
11. Za bezpieczeństwo przetwarzania danych osobowych w określonym procesie indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.
12. W czasie chwilowej nieobecności pracowników w pomieszczeniach, w godzinach pracy jak i po zakończeniu pracy, są oni zobowiązani do zamykania na klucz pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe.
13. Klucze do pomieszczeń, w których przetwarzane są dane osobowe nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia kluczy przed udostępnieniem ich osobom nieupoważnionym.
14. Przed wyjściem z pomieszczenia, w którym przechowywane są dane osobowe należy upewnić się, że zostało ono odpowiednio zabezpieczone (zamknięte okna, drzwi).

15. Po zakończeniu pracy w systemie informatycznym, w którym przechowywane są dane osobowe, należy wylogować się z systemu.
16. Osoba użytkująca komputer przenośny zawierający dane osobowe zobowiązana jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe.
17. Na pracowniku pracującym zdalnie spoczywa obowiązek odpowiedniego zabezpieczenia danych tak, aby osoby trzecie nie miały dostępu do danych osobowych.

16. PRZEGLĄDY I AKTUALIZACJA POLITYKI OCHRONY DANYCH OSOBOWYCH

1. Polityka podlega okresowemu przeglądowi pod kątem jej adekwatności, nie rzadziej niż raz do roku.
2. Przeglądu Polityki dokonuje Administrator Danych.
3. Przegląd powinien obejmować, w szczególności ocenę adekwatności Polityki do:
 - 3.1. procesów funkcjonujących w strukturach Administratora Danych,
 - 3.2. obowiązujących przepisów prawa odnoszących się do ochrony danych osobowych, którym podlega Administrator Danych.
4. W każdym przypadku, gdy zmianie ulegają przepisy prawa będące źródłem wskazanych w Polityce obowiązków lub zaistnieją istotne zmiany faktyczne w ramach struktury Administratora Danych przegląd Polityki wykonywany jest niezwłocznie.
5. Jeżeli w wyniku przeglądu Polityki stwierdzona zostanie konieczność aktualizacji jej zapisów, Administrator Danych dokonuje aktualizacji Polityki w wymaganym zakresie.

17. ZAŁĄCZNIKI

Załącznik nr 1	Zasady retencji danych osobowych
Załącznik nr 2	Procedura szkoleń oraz nadawania upoważnień do przetwarzania danych osobowych
Załącznik nr 3A	Procedura postępowania z naruszeniami ochrony danych osobowych
Załącznik nr 3B	Kalkulacja oceny ryzyka naruszenia
Załącznik nr 4A	Procedura oceny ryzyka dla procesów lub sposobów organizacji przetwarzania danych
Załącznik nr 4B	Matryca oceny ryzyka dla procesów lub sposobów organizacji przetwarzania danych
Załącznik nr 5	Procedura oceny skutków dla ochrony danych osobowych (<i>data protection impact assessment</i>)
Załącznik nr 6	Test równowagi prawnie uzasadnionego interesu (<i>balancing test</i>)
Załącznik nr 7	Procedura realizacji praw osób, których dane dotyczą
Załącznik nr 9	Procedura kontroli podmiotów przetwarzających
Załącznik nr 10	Ogólny opis organizacyjnych środków bezpieczeństwa
Załącznik nr 11	Ogólny opis technicznych środków bezpieczeństwa

Dokument sporządzono: Data: 11/05/2024 Miejsce: Grabowo Wielkie	Administrator Danych
 <i>podpis, pieczęć</i>