

Polityka ochrony danych osobowych

**OVAL SPÓŁKA Z OGRANICZONĄ
ODPOWIEDZIALNOŚCIĄ SPÓŁKI KOMANDYTOWEJ
Z SIEDZIBĄ W MALBORKU**

KRS 0000743006

Maj 2018 r.

Rozdział 1
Postanowienia ogólne.

§ 1

Polityka ochrony danych **OVAL spółka z ograniczoną odpowiedzialnością spółki komandytowej z siedzibą w Malborku**, określa kierunki działań przewidzianych do wykonania oraz sposób ustanowienia zasad i reguł postępowania koniecznych do zapewnienia właściwej ochrony przetwarzanych w Spółce danych.

Polityka obejmuje całokształt zagadnień związanych z zabezpieczeniem danych osobowych przetwarzanych zarówno tradycyjnie jak i w systemach informatycznych. Szczegółowy opis reguł bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych określa Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w **OVAL spółka z ograniczoną odpowiedzialnością spółce komandytowej**, stanowiąca oddzielny dokument.

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – 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 oraz uchylecia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1).

Polityka zawiera:

- a. Opis zasad ochrony danych obowiązujących w Spółce;
- b. Odwołania do załączników uszczegółowiających

Odpowiedzialnym za wdrożenie i utrzymanie niniejszej Polityki w Spółce jest Zarząd Spółki.

Politykę stosuje się również do przetwarzania innych danych, np. dane finansowo-księgowe. **OVAL spółka z ograniczoną odpowiedzialnością spółka komandytowa** realizuje zadania wyłącznie na mocy przepisów prawa uprawniających Administratora Danych Osobowych do przetwarzania danych osobowych.

OVAL spółka z ograniczoną odpowiedzialnością spółka komandytowa dołoży wszelkich starań oraz zapewni odpowiednie środki organizacyjno-finansowe, aby wdrożyć i utrzymywać na odpowiednio wysokim poziomie mechanizmy zabezpieczenia informacji i systemów

informatycznych poprzez dostosowanie działań do wymogów zawartych w obowiązujących przepisach oraz przyjęte dobre praktyki oraz nakazuje ich bezwzględne stosowanie przez pracowników i współpracowników **OVAL spółka z ograniczoną odpowiedzialnością spółki komandytowej** przetwarzających dane osobowe.

Spółka dokumentuje podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

Spółka spełnia wymogi informacyjne względem osób, których dane przetwarza oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym

- a. obowiązki informacyjne. Spółka przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków;
- b. możliwość wykonania żądań. Spółka weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających;
- c. obsługa żądań. Spółka zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany w RODO i udokumentowane;
- d. zawiadamianie o naruszeniach. Spółka stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

§ 2

Ilećroć w Polityce jest mowa o:

1. **Spółce** – rozumie się przez to **OVAL spółka z ograniczoną odpowiedzialnością spółkę komandytową z siedzibą w Malborku**;
2. **Administrator Danych Osobowych lub Administratorze** – rozumie się przez to **OVAL spółka z ograniczoną odpowiedzialnością spółkę komandytową z siedzibą w Malborku**.
3. **Administrator Systemu Informatycznego (ASI)** – rozumie się przez to informatyka, który jest odpowiedzialny za sprawność i konserwację oraz wdrożenie technicznych zabezpieczeń systemów informatycznych w przetwarzanych zbiorach danych osobowych **OVAL spółka z ograniczoną odpowiedzialnością spółki komandytowej**.

4. **danych osobowych** – rozumie się przez to każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby; informacja, która pozwoli na zidentyfikowanie danej osoby,
5. **UODO** – rozumie się przez to Urząd Ochrony Danych Osobowych,
6. **integralności danych osobowych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
7. **osobie trzeciej** - rozumie się przez to każdą osobę nieuprawnioną tj. nieupoważnioną do dostępu do danych osobowych lub zbiorów tych danych,
8. **poufności danych osobowych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
9. **przetwarzaniu danych osobowych** - rozumie się przez to jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie,
10. **rozliczalności danych osobowych** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
11. **sieci lokalnej** – rozumie się przez to połączenie systemów informatycznych **OVAL spółka z ograniczoną odpowiedzialnością spółki komandytowej** wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnej,
12. **systemie informatycznym** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
13. **ustawie** – rozumie się przez to ustawę z dnia 25 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000),
14. **zabezpieczeniu danych osobowych** - rozumie się przez to wdrożenie i eksploatację stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
15. **zbiorze danych osobowych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

§ 3

1. Dane osobowe przetwarzane przez Administratora gromadzone są w zbiorach danych.

2. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzania odbywało się zgodnie z RODO i niniejszą Polityką oraz aby móc to wykazać. Środki te są w razie potrzeby poddawane bieżącej analizie i aktualizowane.
3. Administrator zapewnia stosowanie wdrożonych w Spółce środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości Przetwarzania danych.
4. Administrator prowadzi rejestr czynności przetwarzania danych osobowych za które odpowiada.
5. Rejestr czynności przetwarzania udostępnia się za żądanie Organowi nadzorczemu.
6. Rejestr czynności przetwarzania stanowi załącznik nr 9 do niniejszej Polityki.

§ 4

Polityka bezpieczeństwa ma zastosowanie w przypadku przetwarzania danych osobowych w formie:

1. papierowej tj. kartotek, rejestrów, akt osobowych, skorowidzów, ksiąg, wykazów i innych zbiorów,
2. elektronicznej tj. przetwarzania danych osobowych z użyciem systemu informatycznego oraz urządzeń wchodzących w jego skład.

§ 5

Administrator Danych Osobowych jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych **OVAL spółka z ograniczoną odpowiedzialnością spółki komandytowej**, a w szczególności:

1. zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym,
2. zapobiegać przed zabraniem danych przez osobę trzecią,
3. zapobiegać przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych,
4. nadzorować przestrzeganie zasad technicznej i organizacyjnej ochrony danych osobowych, w tym kontrolowania prawidłowego wykorzystania wdrożonych do stosowania dokumentów wewnętrznych,
5. analizować aktualność dokumentów wewnętrznych Spółki, dotyczących ochrony danych osobowych i przygotowywanie zmian tych dokumentów,

6. zapoznać osoby upoważnione z przepisami ustawy o ochronie danych osobowych i Polityką Ochrony Danych Osobowych OVAL spółka z ograniczoną odpowiedzialnością sp. k., kontrolować pracowników i inne osoby upoważnionych pod względem przetwarzania przez nich danych osobowych,
7. kontrolować pod względem skuteczności stosowania środków fizycznych, sprzętowych i programowych mających na celu zachowanie poufałości, integralności i rozliczalności danych osobowych,
8. kontrolować osoby zajmujące się przechowywaniem i archiwizacją dokumentów zawierających dane osobowe, pod względem prawidłowego ich zabezpieczenia,
9. kontrolować podmioty, którym powierzono przetwarzanie danych osobowych, pod względem prawidłowego ich zabezpieczenia,
10. prowadzić postępowania w przypadku naruszenia ochrony danych osobowych, analizowanie przyczyn naruszenia i przywrócenie stanu prawidłowego.

§ 6

Do zadań **ASI** należy:

1. zapewnienie bezpieczeństwa systemu informatycznego, w którym przetwarzane są dane osobowe, bieżący monitoring i zapewnienie ciągłości pracy systemu,
2. przeciwdziałanie dostępowi do systemu informatycznego osób nieuprawnionych,
3. odpowiedzialność za sprawność, konserwację oraz wdrożenie technicznych zabezpieczeń systemu informatycznego, służącego do przetwarzania danych osobowych,
4. nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym służącym do przetwarzania danych osobowych - nadawanie uprawnień do przetwarzania danych osobowych w postaci identyfikatora użytkownika systemu (login),
5. zapewnienie bezpiecznej wymiany danych w sieci lokalnej oraz nadzór nad przesyłaniem danych za pośrednictwem urządzeń teletransmisji,
6. diagnozowanie zdarzeń i usuwanie awarii sprzętu służącego do przetwarzania danych osobowych,
7. wykonywanie innych zadań wynikających z Polityki.

§ 7

Dane osobowe mogą być przetwarzane wyłącznie przez osoby do tego uprawnione na podstawie upoważnienia wydawanego przez Administratora Danych Osobowych oraz po podpisaniu oświadczenia w nim zawartego.

Wzór upoważnienia stanowi **załącznik nr 2** do Polityki.

Rozdział 2

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.

§ 8

Dane osobowe przetwarzane są w siedzibie Spółki **OVAL spółka z ograniczoną odpowiedzialnością spółki komandytowej** Szczegółowy wykaz pomieszczeń, w których są przetwarzane te dane, zawarty jest w **załączniku nr 1** do Polityki.

W przypadku zaistnienia potrzeby przetwarzania danych osobowych poza siedzibą Spółki, przekazanie danych innemu podmiotowi następuje na podstawie umowy przekazania danych i ze szczególną dbałością o bezpieczeństwo tych danych.

Rozdział 3

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

§ 9

1. Środki organizacyjne ochrony danych osobowych

W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, **OVAL spółka z ograniczoną odpowiedzialnością spółka komandytowa** wprowadza następujące środki organizacyjne:

- 1) przetwarzanie danych osobowych może odbywać się wyłącznie w ramach wykonywania zadań służbowych. Zakres uprawnień wynika z zakresu tych zadań,
- 2) do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające stosowne upoważnienie.

Wzór upoważnienia do przetwarzania danych osobowych stanowi **załącznik nr 2** do niniejszego Polityki.

Dodatkowe uprawnienia (jeżeli ich nadanie będzie potrzebne) do przetwarzania danych osobowych w systemie elektronicznym, określa Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w **OVAL spółka z ograniczoną odpowiedzialnością spółce komandytowej**.

- 4) Administrator Ochrony Danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. Wzór ewidencji stanowi **załącznik nr 3** do niniejszego Polityki,
- 5) zabrania się przetwarzania danych osobowych przez pracowników poza siedzibą **OVAL spółka z ograniczoną odpowiedzialnością spółki komandytowej**,
- 6) każdy upoważniony do przetwarzania danych potwierdza pisemnie fakt zapoznania się z niniejszą Polityką i zrozumienia wszystkich zasad bezpieczeństwa.
Wzór potwierdzenia stanowi **załącznik nr 4** do niniejszego Polityki,
- 7) osoby upoważnione do przetwarzania danych i przebywania w obszarach przetwarzania danych osobowych zobowiązane są zapoznać się z zapisami Polityki i Instrukcji;
wykaz osób, które zostały zapoznane z tymi dokumentami stanowi **załącznik nr 5** do niniejszej Polityki
- 8) obszar przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych,
- 9) pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz,
- 10) monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane,
- 11) przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych należy zamknąć okna oraz usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach lub biurkach.
- 12) przebywanie osób trzecich w obszarze przetwarzania danych osobowych, jest dopuszczalne tylko przez osoby upoważnione przez Administratora Danych Osobowych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
Wzór upoważnienia do przebywania w obszarze przetwarzania danych osobowych stanowi **załącznik nr 6** do Polityki.

2. Środki techniczne ochrony danych osobowych stanowią załącznik nr 7 do Polityki

Dodatkowe środki ochrony technicznej systemu informatycznego, jak również wszystkie niezbędne informacje dotyczące jego pracy oraz zasad użytkowania, określa Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

3. W Spółce obowiązuje również Polityka czystego biurka, haseł, kluczy, której szczegółu określone są w Załączniku nr 12 do Polityki.

§ 10

Zasady przetwarzania danych metodami tradycyjnymi (papierowo)

Przy przetwarzaniu danych w postaci papierowej uwzględnia się następujące zasady:

- 1) dane przetwarzane metodami tradycyjnymi podlegają ochronie na równi ze zbiorami elektronicznymi,
- 2) wszystkie możliwe do wykonania działania dotyczące zbiorów elektronicznych dotyczą również zbiorów papierowych, m. in. wydawanie upoważnień do przetwarzania zbiorów papierowych, zabezpieczenia fizycznego dostępu do szaf i sejfów, w których przechowywane są dane, zwrócenie uwagi na niepozostawianie dokumentów na biurkach, w skanerach czy kserokopiarkach,
- 3) przy naruszeniu zasad bezpieczeństwa zbiorów papierowych obowiązują te same zasady postępowania oraz zgłoszenia incydentu, jak w przypadku naruszenia zasad bezpieczeństwa przy zbiorach elektronicznych.

Spółka zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Spółkę.

Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 11

Każdy pracownik **OVAL spółka z ograniczoną odpowiedzialnością spółki komandytowej**, który stwierdził:

1. naruszenie zawartości zbioru danych osobowych,
2. ujawnienie metod pracy Spółki lub sposobów działania programu w Spółce osobom trzecim,
3. naruszenie bezpieczeństwa systemu informatycznego,
4. naruszenie technicznego stanu urządzeń, służących do przetwarzania danych osobowych,
5. zmianę jakości transmisji danych w sieci telekomunikacyjnej, mogącą wskazywać na naruszenie zabezpieczenia tych danych,
6. zaistnienie innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

obowiązany jest niezwłocznie powiadomić o tym fakcie Administratora Danych Osobowych.

§ 12

W przypadku, gdy niemożliwe jest zgłoszenie naruszenia przetwarzania danych osobowych Administratorowi Danych Osobowych, należy ten fakt zgłosić bezpośrednio przełożonemu. Spółka stosuje procedury powalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych, w terminie 72 godzin od ustalenia naruszenia.

§ 13

Do czasu przybycia Administratora Danych Osobowych na miejsce naruszenia ochrony danych osobowych, należy:

1. niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie w miarę możliwości ustalić przyczyny lub sprawców naruszenia,
2. rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
3. zaniechać (o ile to możliwe) dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę przyczyn, skutków i sprawców naruszenia,
4. podjąć inne działania, odpowiednio dostosowane do zaistniałych okoliczności oraz ich skutków,
5. udokumentować wstępnie zaistniałe naruszenie,
6. nie opuszczać, bez uzasadnionej potrzeby, miejsca zdarzenia do czasu przybycia Administratora Danych Osobowych.

§ 14

W przypadku naruszenia ochrony danych osobowych Administrator Danych poucza i instruuje osoby, które dopuściły się uchybień i dokumentuje zaistniały przypadek sporządzając raport. Wzór raportu stanowi **załącznik nr 8** do niniejszej Polityki.

§ 15

W przypadku, gdy zdarzenie ma charakter przestępstwa, Administrator Danych Osobowych zawiadamia o tym fakcie odpowiednie organy ścigania – Prokuraturę lub Policję.

Rozdział 5

Powierzenie przetwarzania danych osobowych

§ 16

Jeżeli przetwarzanie ma być dokonywane w imieniu Administratora Danych Osobowych, korzysta on z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi Rozporządzenia i chroniło prawa osób, których dane dotyczą.

§ 17

Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej, szczegółowej lub ogólnej pisemnej pod rygorem nieważności zgody Administratora Danych Osobowych. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym Administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.

§ 18

Administrator, powierzając przetwarzanie danych osobowych innemu podmiotowi, zobowiązany jest zawrzeć, na piśmie pod rygorem nieważności, umowę powierzenia przetwarzania danych osobowych, określającą przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa Administratora. Umowa może stanowić odrębny dokument lub jej treść może stanowić część zasadniczej umowy z podmiotem.

§ 19

Administrator nie wyraża zgody, aby podmiot przetwarzający mógł zlecić osobom trzecim (w szczególności podwykonawcom) wykonywanie czynności wymagających podpowierzenia przetwarzania danych osobowych, bez uprzedniej zgody Administratora wyrażonej na piśmie pod rygorem nieważności.

§ 20

Przed powierzeniem przetwarzania danych osobowych Administrator, w miarę możliwości, uzyskuje informacje o dotychczasowych praktykach przetwarzającego, dotyczących danych osobowych.

§ 21

Wzór umowy powierzenia danych określa **Załącznik nr 10** do niniejszej Polityki.

§ 22

1. Spółka informuje osobę o przetwarzaniu jej danych przy pozyskaniu danych od tej osoby.
2. Spółka informuje osobę o planowanej zmianie celu przetwarzania danych.
3. Spółka informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych.
4. Spółka bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw i wolności tej osoby.

§ 23

Spółka dba o minimalizację przetwarzania danych pod kątem adekwatności danych do celów (ilości danych i zakresu przetwarzania), dostępu do danych oraz czasu przechowywania danych.

§ 24

W sprawach nieuregulowanych postanowieniami niniejszej Polityki zastosowanie mają postanowienia rozporządzenia RODO oraz ustawy o ochronie danych osobowych.

§ 25

Wszelkie zmiany niniejszej Polityki mogą być dokonywane w każdym czasie przez komplementariusza Spółki i wchodzi w życie z dniem ich podania do wiadomości publicznej.