ZARZĄDZENIE nr _

Prezesa Windbud Sp z o.o.

z dnia 25 maja 2018 r.

w sprawie wprowadzenia Polityki ochrony danych wraz z politykami towarzyszącymi

Na podstawie art. 24 ust. 2 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) (Dz. Urz. UE, L 119 z 4.05.2016)

zarządzam co następuje:

§1

Wprowadza się w Windbud Sp z o.o. Politykę ochrony danych wraz z politykami i zasadami towarzyszącymi, w brzmieniu określonym w Załączniku nr 1 do niniejszego zarządzenia.

§2

Polityki towarzyszące, o których mowa w §1 to:

1. Polityka zarządzania systemami informatycznymi.
2. Polityka zarządzania incydentami.
3. Zasady prowadzenia analizy ryzyka.
4. Zasady przetwarzania danych w imieniu administratora.

§3

Treść dokumentów wymienionych w §1 i §2 stanowi przedmiot tajemnicy służbowej.

§4

Zarządzenie wchodzi w życie z dniem podpisania.

.....

.....

podpis Prezesa

Windbud Sp z o.o.

POLITYKA OCHRONY DANYCH

STANOWIĄCA TAKŻE

POLITYKĘ BEZPIECZEŃSTWA INFORMACJI

1. Deklaracja stosowania

Jednym z głównych zadań naszej organizacji jest zapewnienie ochrony przetwarzanych danych z zachowaniem gwarancji należytego bezpieczeństwa i poufności powierzonych informacji.

W celu spełnienia powyższej deklaracji Dyrekcja przyjmuje następującą Politykę ochrony danych, stanowiącą jednocześnie Politykę bezpieczeństwa informacji:

1. Jesteśmy świadomi ważności przetwarzanych w naszej organizacji informacji i będziemy stwarzać odpowiednie warunki dla ich ochrony, w tym także poprzez zabezpieczenie odpowiednich zasobów finansowych i ludzkich.

2. Zobowiązujemy się do spełnienia wymogów prawnych, w szczególności w zakresie wymagań polskich i europejskich przepisów o ochronie danych osobowych, w szczególności RODO.

3. W jednostce funkcjonuje system ochrony danych, zbudowany w oparciu o wymogi RODO oraz uwzględniający wytyczne normy PN ISO/IEC 27001. Zakresem ochrony objęte są wszystkie informacje przetwarzane w placówce, niezależnie od miejsca i sposobu ich przetwarzania.

4. W szczególny sposób zwracamy uwagę na dane osobowe, dokładając szczególnej staranności przy ich przetwarzaniu i ochronie.

5. Za bezpieczeństwo informacji w placówce odpowiada każdy na swoim stanowisku pracy. Zakresy obowiązków pracowników na stanowiskach o szczególnym znaczeniu dla bezpieczeństwa danych obejmują obowiązki związane z ochroną danych.

6. Na podstawie niniejszej Polityki oraz polityki i zasady jej towarzyszące sformułowano procedury i inne zabezpieczenia.

7. Zarządzanie bezpieczeństwem informacji, w tym bezpieczeństwem danych osobowych oparte jest o podejście bazujące na ryzyku. Analiza ryzyka jest kluczowym elementem tworzenia, utrzymania i doskonalenia zabezpieczeń.

8. Obowiązkiem pracowników jest przestrzeganie zasad postępowania opisanych w niniejszej Polityce oraz wszystkich funkcjonujących w placówce polityk, zasad i procedur związanych z bezpieczeństwem.

9. Wdrożony system ochrony danych będzie stale doskonalony.

Niniejsza Polityka wraz z politykami i zasadami jej towarzyszącymi została ogłoszona w jednostce i jest dostępna dla wszystkich pracowników. Jej treść stanowi przedmiot tajemnicy służbowej.

Treść niniejszej Polityki wraz z towarzyszącymi jej dokumentami jest elementem formalno-organizacyjnych zabezpieczeń danych i ma charakter poufny. Ujawnienie jej treści osobom trzecim może przyczynić się do obniżenia poziomu bezpieczeństwa danych i informacji w jednostce. W związku z tym dokumenty te nie podlegają publikacji w Biuletynie Informacji Publicznej.

Dyrekcja placówki deklaruje pełne zaangażowanie w realizację postanowień niniejszej Polityki.

Bydgoszcz, 25 maj 2018

.....

pieczęć i podpis dyrektora

2. Analiza ryzyka

Analiza ryzyka jest fundamentem tworzenia, utrzymania i doskonalenia zabezpieczeń.

Analizę ryzyka prowadzi się zgodnie z *Zasadami prowadzenia analizy ryzyka*, zawartymi w odrębnym dokumencie.

Plik - **Analiza ryzyka WINDBUD.xlsx**

3. Rejestr czynności przetwarzania

Wymogi

W jednostce prowadzi się Rejestr czynności przetwarzania, zgodnie z wymogami art. 30 ust. 1 RODO.

Prowadzony rejestr obejmuje następujące informacje:

- numer wpisu w rejestrze,
- określenie zbioru danych, którego dotyczy dana czynność,
- określenie czynności przetwarzania,
- datę wpisu czynności do rejestru,
- datę ostatniej modyfikacji wpisu czynności w rejestrze,
- informację, czy czynność obejmuje przetwarzanie danych w formie papierowej,
- informację o pomieszczeniach, w których przetwarza się dane w formie papierowej,
- informację o klasyfikacji grupy ryzyka dokumentów papierowych,
- kategorie osób, których dane dotyczą,
- kategorie danych osobowych w odniesieniu do każdej kategorii osób,
- podstawę prawną przetwarzania danych (odrębnie dla danych zwykłych i danych szczególnie chronionych, tzw. „wrażliwych”),
- wskazanie szczegółowej podstawy prawnej w przypadku, gdy przetwarzanie odbywa się na podstawie przesłanki określonej w art. 6 ust. 1 lit. c) lub art. 9 ust. 2 lit. a) RODO,
- cel przetwarzania danych,
- planowany termin usunięcia danych,
- kategorie odbiorców, którym dane mogą być udostępniane,
- nazwę, adres i kontakt do współ administratorów,
- podstawę prawną do transferu danych do państwa trzeciego,
- informację o przeprowadzeniu oceny skutków dla ochrony danych.

Realizacja

Rejestr czynności przetwarzania prowadzi się w formie elektronicznej.

Forma prowadzenia rejestru umożliwia sporządzenie z niego wydruku.

Plik - **Rejestr_czynnosci_przetwarzania_Windbud.xlsx**

4. Systemy informatyczne używane do ich przetwarzania

Wykaz systemów informatycznych wykorzystywanych do przetwarzania danych osobowych

W organizacji wykorzystywane są następujące systemy informatyczne, w których przetwarza się dane osobowe:

Nazwa systemu	Nazwa programów w ramach tego systemu	Czy służy do wprowadzania danych osobowych?
Płatnik	Płatnik ZUS	tak
Comarch™ Optima	Comarch ERP Optima księgowość	tak
Excel	rejestry w postaci tabel	nie
	…	tak/nie
…	…	tak/nie

5. Organizacja bezpieczeństwa informacji

Organizacja wewnętrzna

Zaangażowanie kierownictwa w bezpieczeństwo informacji

Koordynacja bezpieczeństwa informacji

Przypisanie odpowiedzialności w zakresie bezpieczeństwa informacji

Proces autoryzacji środków przetwarzania informacji

Umowy o zachowaniu poufności

Kontakty z organami władzy

Kontakty z grupami zaangażowanymi w zapewnienie bezpieczeństwa

Niezależny przegląd bezpieczeństwa informacji

Strony zewnętrzne

6. Zarządzanie aktywami

Inwentaryzacja aktywów

Własność aktywów

Akceptowalne użycie aktywów

7. Bezpieczeństwo zasobów ludzkich

Przed zatrudnieniem

Role i zakresy odpowiedzialności

Postępowanie sprawdzające

Zasady i warunki zatrudnienia

Podczas zatrudnienia

Odpowiedzialność kierownictwa

Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji

Postępowanie dyscyplinarne

Zakończenie lub zmiana zatrudnienia

Odpowiedzialność związana z zakończeniem zatrudnienia

Zwrot aktywów

Odebranie praw dostępu

8. Bezpieczeństwo fizyczne i środowiskowe

Obszary bezpieczne

Fizyczne granice obszaru bezpiecznego

Fizyczne zabezpieczenie wejścia

Nadzór wejść

Zabezpieczanie pomieszczeń

Ochrona przed zagrożeniami zewnętrznymi i środowiskowymi

Praca w obszarach bezpiecznych

Obszary publicznie dostępne

Zabezpieczenia obszaru przetwarzania danych osobowych

Szczególną wagę w działalności jednostki przykłada się do bezpieczeństwa danych osobowych. W związku z tym zabezpieczenia obszaru przetwarzania danych osobowych podlegają odrębnej analizie i dodatkowym uregulowaniom.

Stosuje się niżej opisane zabezpieczenia obszaru przetwarzania danych osobowych.

Składowa obszaru przetwarzania danych osobowych	Określenie stosowanych zabezpieczeń
Siedziba firmy (biuro - wynajmowane pomieszczenie)	**Drzwi**: standardowe **Zamki**: standardowe **Kraty w oknach**: nie **Alarm**: nie **Monitoring**: nie
Siedziba firmy (wejście do budynku)	**Drzwi**: wzmocnione **Zamki**: elektroniczne: karta/kod **Kraty w oknach**: nie **Alarm**: tak **Monitoring**: tak

Bezpieczeństwo sprzętu

Lokalizacja i ochrona sprzętu

Systemy wspomagające

Bezpieczeństwo okablowania

Konserwacja sprzętu

Bezpieczeństwo sprzętu poza siedzibą

Bezpieczne zbywanie sprzętu lub przekazywanie do ponownego użycia

Wynoszenie mienia

9. Zarządzanie systemami i sieciami

Zasady obowiązujące w zakresie zarządzania systemami i sieciami w jednostce zostały opisane w odrębnym dokumencie, zatytułowanym *Polityka zarządzania systemami informatycznymi*, który stanowi integralny element niniejszej Polityki ochrony danych.

10. Kontrola dostępu

Wymagania wobec kontroli dostępu

Polityka kontroli dostępu

Zarządzanie dostępem użytkowników

Dostęp do systemów informatycznych

Zasady zarządzania dostępem użytkowników do wykorzystywanych w jednostce systemów informatycznych zostały uregulowane w dokumencie *Polityka zarządzania systemami informatycznymi*.

Dostęp do budynku

Dostęp do kluczy

W organizacji klucze do pomieszczeń dzieli się na klucze wykorzystywane operacyjnie oraz klucze awaryjne (zapasowe).

Szczegółowe zasady dostępu do kluczy określono poniżej.

Klucze do biura	Miejsce i sposób przechowywania	Czy wydawanie jest ewidencjonowane?	Własne kopie kluczy posiadają
Kamila Chmara	klucze operacyjne brak kluczy zapasowych klucze nie są wydawane	nie	brak

Odpowiedzialność użytkowników

Polityka czystego biurka i czystego ekranu

Kontrola dostępu do sieci

Uregulowania dotyczące zasad dostępu do sieci znajdują się w dokumencie *Polityka zarządzania systemami informatycznymi*.

11. Zarządzanie incydentami związanymi z bezpieczeństwem informacji

Obowiązujące w jednostce zasady w zakresie zarządzania incydentami związanymi z bezpieczeństwem informacji zostały uregulowane w *Polityce zarządzania incydentami*.

Plik - **Rejestr_incydentow_Windbud.xlsx**

12. Zarządzanie ciągłością działania

13. Udostępnianie danych

Zgodnie z obowiązującymi uregulowaniami prawnymi udostępnianie danych jest jedną z form ich przetwarzania. W związku z tym udostępnianie danych następuje każdorazowo po weryfikacji podstawy prawnej legalizującej wykonanie tej operacji.

Dane, dla których administratorem danych w rozumieniu przepisów ustawy o ochronie danych osobowych jest jednostka udostępnia się:

- podmiotom, którym obowiązek udostępniania danych wynika z przepisów prawa – po weryfikacji obowiązywania tych przepisów,
- innym podmiotom:
    - po złożeniu pisemnego wniosku o udostępnienie danych,
    - po weryfikacji podstawy prawnej udostępnienia danych na podstawie złożonego wniosku,
- podmiotom, z którymi zawarto umowę, dla realizacji której niezbędne jest udostępnienie danych, po weryfikacji treści zapisów umowy.

Decyzję o udostępnieniu danych lub odmowie ich udostępnienia podejmuje Dyrektor jako administrator danych, po zasięgnięciu opinii Inspektora ochrony danych.

14. Monitoring wizyjny - brak

Stosowanie monitoringu wizyjnego

Zakres monitorowania

Zasady gromadzenia zapisu monitoringu

Udostępnianie danych z zapisu monitoringu

18. Przeglądy polityki i audyty systemu bezpieczeństwa

Windbud Sp z o.o.

POLITYKA ZARZĄDZANIA SYSTEMAMI INFORMATYCZNYMI

Spis treści

Polityka określa zasady zarządzania systemami informatycznymi wykorzystywanymi w Windbud Sp. z o.o.

Treść niniejszej Polityki stanowi przedmiot tajemnicy służbowej dla wszystkich pracowników i współpracowników jednostki.

1. Deklaracja stosowania

Nasza organizacja w swojej działalności wykorzystuje systemy informatyczne, przetwarzające dane, w tym dane osobowe. Jednym z naszych głównych celów jest zapewnienie bezpieczeństwa przetwarzanych danych. W tym celu stosuje się szereg środków zabezpieczających, dobranych adekwatnie do zagrożeń.

Przedmiotem szczególnej uwagi jest zagadnienie przetwarzania danych osobowych i zagwarantowanie tym danym jak najwyższego poziomu bezpieczeństwa.

W celu realizacji przyjętej polityki bezpieczeństwa przyjmuje się i wdraża niniejszą *Politykę*. Dyrekcja deklaruje pełne zaangażowanie w realizację niniejszej *Polityki*.

2. Postanowienia ogólne

Polityka zarządzania systemami informatycznymi składa się z części ogólnej oraz może zostać uzupełniona o część szczegółową. Zasady zawarte w części ogólnej obowiązują w odniesieniu do wszystkich systemów informatycznych wykorzystywanych w jednostce. W części szczegółowej mogą być zawarte dodatkowe uregulowania, specyficzne dla poszczególnych systemów, jeżeli są wymagane. O rozbudowaniu *Polityki* o część szczegółową decyduje Dyrektor w porozumieniu z Inspektorem Ochrony Danych oraz administratorem systemu informatycznego.

Polityka reguluje zasady zarządzania systemami informatycznymi oraz podstawowe zasady użytkowania tych systemów.

3. Odpowiedzialność

Za zarządzanie systemami informatycznymi w organizacji odpowiedzialny jest administrator systemu informatycznego lub inna osoba wykonująca jego obowiązki.

Zakres czynności realizowanych przez administratora systemu informatycznego regulują: niniejsza *Polityka*, *Polityka Bezpieczeństwa Informacji* oraz indywidualne zakresy obowiązków osób pełniących tę funkcję.

Dopuszcza się tworzenie procedur i instrukcji szczegółowych, precyzujących postanowienia niniejszej *Polityki*. Procedury i instrukcje szczegółowe nie mogą przewidywać rozwiązań zmniejszających poziom bezpieczeństwa określony w niniejszej *Polityce*. W przypadku sprzeczności uregulowań pierwszeństwo stosowania ma zawsze niniejsza *Polityka*.

Administrator systemu informatycznego jest zobowiązany do ścisłej współpracy z Inspektorem Ochrony Danych.

Nadzór nad działalnością administratora systemu informatycznego sprawuje Dyrekcja we współpracy z Inspektorem Ochrony Danych.

4. Dostęp do systemu

Dostęp do dowolnego systemu informatycznego funkcjonującego w Windbud Sp z o.o może otrzymać tylko osoba upoważniona do przetwarzania danych znajdujących się w tym systemie.

Jeżeli w systemie przetwarzane są dane osobowe, dostęp do systemu może być udzielony po uzyskaniu przez daną osobę upoważnienia do przetwarzania danych osobowych wystawionego przez administratora danych – zgodnie z obowiązującymi w tym zakresie zasadami opisanymi w dokumencie *Polityki bezpieczeństwa informacji* – oraz dokonania wpisu w ewidencji osób upoważnionych do przetwarzania danych osobowych.

Jeżeli system informatyczny jest wykorzystywany przez więcej niż jedną osobę, dostęp do niego wymaga identyfikacji użytkownika i jego uwierzytelnienia, a użytkownikowi przydziela się identyfikator oraz hasło.

Zasady konstrukcji identyfikatorów określa administrator systemu informatycznego w porozumieniu z Inspektorem Ochrony Danych. Administrator systemu informatycznego jest odpowiedzialny za prowadzenie dokumentacji dotyczącej nadanych identyfikatorów w sposób umożliwiający w dowolnej chwili uzyskanie jednoznacznej informacji kto personalnie używa danego identyfikatora oraz jakie identyfikatory używane są przez daną osobę.

Dopuszcza się, by wobec systemów przetwarzających dane osobowe rolę dokumentacji, o której mowa powyżej pełniła ewidencja osób upoważnionych do przetwarzania danych osobowych, pod warunkiem, że spełnia wyżej wymienione wymagania.

Identyfikator w postaci określonego ciągu znaków w danym systemie informatycznym może być przydzielony tylko jednej osobie. Identyfikator raz użyty nie może być użyty ponownie, również w sytuacji, w której osoba już nie pracuje w systemie. Bezwzględnie zabrania się tworzenia w systemach informatycznych kont wspólnych – użytkowanych przez więcej niż jedną osobę.

5. Nadawanie uprawnień

Uprawnienia do pracy w systemie nadaje administrator systemu informatycznego lub osoba wykonująca jego obowiązki na wniosek Dyrekcji.

Uprawnienie do pracy w systemie informatycznym przetwarzającym dane osobowe może być nadane wyłącznie osobie, która posiada upoważnienie do przetwarzania danych osobowych nadane przez administratora danych.

Użytkownicy dopuszczani do eksploatacji systemów informatycznych powinni przed rozpoczęciem pracy z systemem zostać zapoznani z wymaganiami nakładanymi na nich przez funkcjonującą w jednostce *Politykę bezpieczeństwa* oraz niniejszą *Politykę zarządzania systemami informatycznymi*, a także pozostałymi uregulowaniami dotyczącymi bezpieczeństwa przetwarzania danych w jednostce.

Użytkownicy dopuszczani do eksploatacji systemów informatycznych przetwarzających dane osobowe powinni zostać ponadto przeszkoleni w zakresie obowiązujących i dotyczących ich przepisów w zakresie ochrony danych osobowych oraz odpowiedzialności z tym związanej.

Po utworzeniu konta w systemie informatycznym przetwarzającym dane osobowe, administrator systemu informatycznego jest zobowiązany upewnić się, że nadany nowemu użytkownikowi identyfikator jest zgodny z wpisanym w ewidencji osób upoważnionych do przetwarzania danych osobowych, a w razie potrzeby zgłosić potrzebę uzupełnienia bądź poprawienia wpisu.

Przy udostępnianiu informacji o koncie jego użytkownikowi, administrator systemu informatycznego jest zobowiązany poinformować użytkownika, czy w danym systemie przetwarzane są dane osobowe.

6. Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

Rozpoczęcie pracy w systemie

Każdy użytkownik przed rozpoczęciem procesu zgłoszenia się w systemie jest zobowiązany sprawdzić stan urządzeń systemu informatycznego oraz swojego stanowiska pracy pod kątem potencjalnych działań stanowiących naruszenie zasad bezpieczeństwa lub próby uzyskania nielegalnego dostępu do danych, zwłaszcza danych osobowych.

W przypadku stwierdzenia nieautoryzowanych działań lub podejrzenia ich podjęcia użytkownik przerywa procedurę rozpoczęcia pracy w systemie, w szczególności nie wykonuje procedury uwierzytelnienia w systemie (nie podaje identyfikatora ani hasła). W tej sytuacji użytkownik jest zobowiązany podejmować działania zgodnie z zasadami postępowania w przypadku podejrzenia wykrycia incydentu lub naruszenia zasad ochrony danych i informacji opisanych w *Polityce bezpieczeństwa informacji*. W przypadku jakichkolwiek wątpliwości użytkownik powinien zgłosić się do Inspektora Ochrony Danych, administratora systemu informatycznego lub swojego bezpośredniego przełożonego.

Jeżeli stan urządzeń oraz stanowiska pracy użytkownika nie budzą jego zastrzeżeń, użytkownik rozpoczyna procedurę uwierzytelnienia w systemie. W trakcie realizacji tej procedury użytkownik jest obowiązany zwrócić szczególną uwagę na informacje poufne, w szczególności zapewnić, by nie dostały się one w posiadanie osób trzecich (na przykład poprzez podejrzenie hasła, wykonanie kopii karty magnetycznej itp.).

Zawieszenie pracy w systemie

Jeżeli użytkownik zamierza chwilowo opuścić stanowisko pracy jest zobowiązany do wykonania czynności uniemożliwiających osobom niepowołanym na dostęp do danych. W szczególności użytkownik opuszczając chwilowo swoje stanowisko pracy jest zobowiązany do zapisania danych, na których pracuje, a następnie do

zablokowania stacji roboczej z wykorzystaniem mechanizmów systemu operacyjnego lub oprogramowania. Zablokowanie stacji roboczej oznacza wprowadzenie systemu informatycznego w stan, w którym kontynuacja pracy przez danego użytkownika możliwa jest dopiero po ponownym jego uwierzytelnieniu.

Bezwzględnie zabrania się opuszczania stanowiska pracy bez zablokowania dostępu do stacji roboczej.

Zakończenie pracy w systemie

Kończąc pracę w systemie użytkownik jest zobowiązany do zapisania danych, na których pracował, zamknięcia wykorzystywanych programów oraz wykonania operacji wylogowania się z systemu.

Zanim użytkownik opuści swoje stanowisko pracy jest obowiązany upewnić się, że operacja wylogowania się z systemu została wykonana skutecznie.

Ponadto opuszczając stanowisko pracy użytkownik jest zobowiązany do zabezpieczenia przed niepowołanym dostępem podczas jego nieobecności wszelkich dokumentów oraz nośników danych zawierających informacje podlegające ochronie, w szczególności zaś te, na których znajdują się dane osobowe.

7. Uwierzytelnianie w systemie

Do uwierzytelnienia użytkownika w systemie standardowo stosuje się identyfikator oraz hasło. Dla wybranych systemów informatycznych możliwe jest stosowanie innych metod uwierzytelniania (np. karty magnetyczne, karty zbliżeniowe, dane biometryczne). Stosowanie niestandardowych metod uwierzytelniania proponuje administrator systemu informatycznego, opiniuje Inspektor Ochrony Danych a zatwierdza Dyrektor.

Identyfikator zapewnia możliwość jednoznacznego przypisania konta do jego właściciela oraz jest związany z uprawnieniami w systemie. Hasło zapewnia możliwość korzystania z danego konta wyłącznie przez jego właściciela. Identyfikator oraz hasło, wraz z funkcjonalnościami systemów informatycznych są narzędziami zapewniającymi poufność, integralność i rozliczalność przetwarzanych danych.

Dla zachowania wysokiego poziomu bezpieczeństwa użytkownik powinien zachowywać poufność identyfikatorów, którymi się posługuje.

Użytkowników obowiązuje bezwzględny zakaz ujawniania oraz zapisywania haseł.

8. Stosowanie haseł

Hasła stosowane przez użytkowników objęte są tajemnicą służbową i powinny być znane wyłącznie ich właścicielom. Ponadto hasło nie powinno być ujawniane również po utracie jego ważności.

Zabrania się stosowania mechanizmów zapamiętywania haseł w programach, w tym stosowania automatycznych mechanizmów logowania do systemu.

Hasła stosowane przez użytkowników powinny, dla zapewnienia odpowiedniego poziomu bezpieczeństwa, być w odpowiednim stopniu skomplikowane. Hasła do systemów informatycznych przetwarzających dane osobowe powinno składać się co najmniej z ośmiu znaków, w tym co najmniej jedna wielka litera, co najmniej jedna mała litera oraz co najmniej jedna cyfra lub znak specjalny. Zaleca się, by hasła do systemów innych niż te przetwarzające dane osobowe również posiadały wyżej wymieniony minimalny stopień skomplikowania.

Stosowane hasło nie może być takie samo jak identyfikator.

Hasła nie powinny być stosowane wielokrotnie. W przypadku gdy użytkownik posiada konta w wielu systemach informatycznych zaleca się stosowanie różnych haseł w każdym z systemów.

Użytkownik jest zobowiązany zmieniać swoje hasła nie rzadziej niż co 90 dni. Brak wymuszenia przez system informatyczny regularnej zmiany hasła nie zwalnia użytkownika z obowiązku dokonywania jego zmian z ww. częstotliwością.

Z wyjątkiem ewentualnie wykorzystywanych tymczasowych haseł startowych, hasła powinny być tworzone samodzielnie przez użytkownika.

W przypadku wykorzystywania tymczasowych haseł startowych administrator systemu informatycznego jest zobowiązany do przekazywania tych haseł użytkownikom w sposób bezpieczny, zapewniający ich poufność i gwarantujący, że hasło trafia do właściwej osoby. Po pierwszym użyciu takiego hasła powinno ono zostać zmienione przez użytkownika.

Hasła nie mogą być ujawniane ani przekazywane osobom trzecim.

Użytkownik jest w pełni odpowiedzialny za stosowanie swojego hasła oraz za wszystkie czynności dokonane w systemie przy jego wykorzystaniu.

9. Ogólne zasady eksploatacji systemów

Dyrekcja jednostki wraz z administratorem systemu informatycznego oraz Inspektorem Ochrony Danych podejmują działania mające na celu zapewnienie jak najwyższego stopnia bezpieczeństwa dla danych i informacji podczas eksploatacji wykorzystywanych w organizacji systemów informatycznych. Szczególna uwaga przykładana jest do tych systemów, w których przetwarzane są dane osobowe.

Za prowadzenie bieżących, operacyjnych działań w zakresie zarządzania systemami informatycznymi odpowiedzialny jest administrator systemu informatycznego. Wszyscy użytkownicy są zobowiązani do stosowania się do zaleceń wydawanych przez administratora systemu informatycznego.

Użytkownikowi nie wolno instalować oprogramowania, w tym jego aktualizacji, a także wprowadzać zmian do konfiguracji sprzętu lub oprogramowania bez zezwolenia administratora systemu informatycznego.

Użytkownikowi nie wolno samodzielnie podłączać do infrastruktury informatycznej w jednostce prywatnych urządzeń. Podłączenie prywatnego urządzenia może mieć miejsce wyłącznie za zgodą Dyrekcji i powinno być wykonane przez administratora systemu informatycznego, przez wskazaną przez niego osobę lub za jego zgodą przez użytkownika. Szczegółowe uregulowania w tym względzie zawarte są w części *Wykorzystywanie sprzętu prywatnego pracowników*.

Użytkownicy są zobowiązani do przechowywania wykorzystywanych przez siebie danych wyłącznie w miejscach do tego przeznaczonych. Zabrania się przechowywania danych podlegających ochronie, a w szczególności danych osobowych, w miejscach, do których mogą mieć dostęp nieuprawnieni użytkownicy, zwłaszcza w folderach wspólnych lub publicznych.

Użytkownicy nie są uprawnieni do testowania zabezpieczeń systemu informatycznego i jego podatności na różnego rodzaju ataki. Tego typu działania traktowane będą jako próba uzyskania nielegalnego dostępu do systemu i mogą wiązać się z odpowiedzialnością dyscyplinarną i karną.

Użytkownik jest uprawniony do wykorzystywania systemu informatycznego wyłącznie dla celów realizacji swoich obowiązków służbowych. Wykorzystywanie systemu do innych celów wymaga uzyskania zgody bezpośredniego przełożonego lub Dyrekcji.

10. Sprzęt

Sprzęt wchodzący w skład systemów informatycznych wykorzystywanych w jednostce jest dobierany adekwatnie do celu jego wykorzystywania, z uwzględnieniem możliwości ekonomicznych organizacji. W przypadku wątpliwości w doborze sprzętu administrator systemu informatycznego lub Dyrekcja korzystają z pomocy konsultantów zewnętrznych.

Użytkownik jest zobowiązany zgłaszać administratorowi systemu informatycznego lub swojemu bezpośredniemu przełożonemu wszelkie nieprawidłowości w działaniu wykorzystywanego przez niego sprzętu.

Ekrany monitorów powinny być ustawione w sposób uniemożliwiający podejrzenie danych na nich wyświetlanych przez osoby niepowołane, w szczególności przez osoby postronne wchodzące do pomieszczenia, w którym znajduje się stanowisko pracy. Należy zwrócić ponadto uwagę na możliwość podejrzenia ekranu monitora z zewnątrz pomieszczenia, na przykład przez okno.

Infrastruktura sieci teleinformatycznej powinna być zabezpieczona przed nieuprawnionym dostępem i modyfikacjami. W szczególności dotyczy to szaf i pomieszczeń, w których znajdują się zbiorcze zakończenia sieci i urządzenia typu koncentrator.

Struktura sieci teleinformatycznej powinna być udokumentowana.

W przypadku, gdy gniazda sieci elektroenergetycznej są oznakowane, sprzęt komputerowy powinien być podłączany wyłącznie do gniazd oznaczonych jako przystosowane do tego celu. Jeżeli gniazda sieci elektroenergetycznej nie są oznakowane, przy podłączaniu urządzeń komputerowych należy upewnić się, że gniazdo posiada uziemienie oraz właściwą wartość napięcia zasilającego. Zabrania się podłączania stacjonarnego sprzętu komputerowego do gniazd nieposiadających uziemienia.

11. Oprogramowanie

W jednostce wykorzystuje się jedynie legalne, licencjonowane oprogramowanie. Użytkownicy, każdorazowo przy wdrażaniu nowego rozwiązania, powinni zostać poinformowani o postanowieniach umowy licencyjnej. Dotyczy to szczególnie sytuacji, gdy umowa licencyjna na dane oprogramowanie przewiduje nietypowe uregulowania.

Decyzje w zakresie strategii wykorzystywanego oprogramowania podejmuje Dyrektor. O instalacji oprogramowania na poszczególnych stanowiskach decyduje administrator systemu informatycznego w porozumieniu z Dyrekcją.

Użytkownikom nie wolno samodzielnie, bez zgody administratora systemu informatycznego, instalować oprogramowania. Zakaz ten dotyczy również oprogramowania udostępnianego w ramach licencji typu freeware (nieodpłatnie).

Użytkownicy na stacjach roboczych powinni stosować wygaszacze ekranów zabezpieczone hasłem. Czas aktywacji powinien być akceptowalnie jak najmniejszy. Zalecany czas aktywacji wygaszacza, to 10 minut.

Zaleca się przechowywanie wersji instalacyjnych wcześniejszych wersji oprogramowania. Okres przechowywania wersji instalacyjnych starszych wersji używanego oprogramowania powinien być wyznaczany indywidualnie dla każdego programu, z uwzględnieniem potencjalnej potrzeby przywrócenia pracy na danej wersji. Zarządzanie przechowywaniem ww. wersji instalacyjnych jest elementem zarządzania ciągłością działania. Pracami tymi kieruje administrator systemu informatycznego.

Procedura instalacji i wdrożenia nowego oprogramowania lub nowszej wersji wykorzystywanego oprogramowania powinna w przypadku niepowodzenia tych działań zapewniać możliwość przywrócenia wersji poprzedniej.

Logi systemowe i inne pliki zawierające ewidencje zdarzeń w systemach powinny zostać zabezpieczone przed nieautoryzowanym dostępem i modyfikacją. Administrator systemu informatycznego powinien ponadto regularnie kontrolować stan synchronizacji zegarów systemowych we wszystkich elementach systemów, celem zapewnienia rzetelności logów.

12. Kopie zapasowe

W celu zabezpieczenia przed potencjalną utratą danych w jednostce regularnie wykonuje się kopie zapasowe danych.

Administrator systemu informatycznego, w konsultacji z Inspektorem Ochrony Danych jest odpowiedzialny za kreowanie i realizację polityki zarządzania kopiami zapasowymi. Uregulowania zasad postępowania dotyczących kopii zapasowych znajdują się w niniejszej *Instrukcji* oraz w szczegółowych dokumentach, które mogą być wydane przez Dyrekcję, Inspektora Ochrony Danych lub administratora systemu informatycznego, jednakże żadne uregulowanie zawarte w tych dokumentach nie może być sprzeczne z zasadami opisanymi w niniejszej *Polityce*.

Kopie danych oraz kopie kompletnych zbiorów danych może wykonywać wyłącznie administrator systemu informatycznego lub upoważniona przez niego osoba.

Kopie danych zgromadzonych na lokalnych stacjach roboczych mogą być wykonywane przez użytkowników jedynie gdy zachodzi taka realna potrzeba i jedynie w zgodzie z zasadami opisanymi w niniejszej *Instrukcji* i ewentualnych obowiązujących dokumentach uszczegóławiających.

Kopie danych powinny być wykonywane na nośnikach adekwatnych do ilości zabezpieczanych danych i oczekiwanego sposobu dostępu do nich, z uwzględnieniem cech danego typu nośnika, zwłaszcza jego trwałości i podatności na uszkodzenia. Decyzję o wyborze nośników wykorzystywanych do wykonywania kopii danych podejmuje administrator systemu informatycznego.

Nośniki zawierające kopie zapasowe powinny być opisane w sposób jednoznacznie identyfikujący ich zawartość. Administrator systemu informatycznego określa stosowany, ujednolicony sposób opisywania nośników z kopiami zapasowymi.

Podstawowe zasady tworzenia kopii zapasowych ze zbiorów danych osobowych wraz z ich charakterystyką przedstawia poniższa tabela.

Rodzaj danych / System	Częstotliwość wykonywania	Sposób	Nośnik	Miejsce przechowyw.	Okres przechowyw.
laptop w biurze	1 raz na /mies	ręcznie / automat.	dysk sieciowy QNAP	QNAP NAS siedziba firmy	do wykonania kolejnej /
laptop prezesa	1 raz na /mies	ręcznie / automat.	dysk sieciowy QNAP	QNAP NAS siedziba firmy	do wykonania kolejnej /

Administrator systemu informatycznego czuwa nad realizacją tworzenia kopii zapasowych wedle przedstawionych powyżej zasad. Administrator systemu informatycznego ma ponadto prawo do wprowadzania doraźnych zmian w zakresie zasad tworzenia kopii opisanych w powyższej tabeli, jeśli uzna je za służące zapewnieniu odpowiedniego poziomu bezpieczeństwa danych.

Do niszczenia kopii zapasowych stosuje się zapisy dotyczące usuwania danych zawarte w niniejszej *Instrukcji*.

13. Nośniki danych

Rodzaje używanych nośników danych

W organizacji dopuszcza się do użytku następujące rodzaje nośników danych:

- dyski twarde serwerów,
- dyski twarde komputerów stanowiących stacje robocze (w tym komputerów przenośnych),
- optyczne nośniki danych (CD/DVD/Blue ray)
- nośniki przenośne typu pendrive,
- zewnętrzne (internetowe) systemu przechowywania danych.

Wykorzystywanie nośników danych

Podstawowym nośnikiem przechowywania danych, które są na bieżąco wykorzystywane w pracy jednostce są dyski twarde serwerów oraz dyski twarde komputerów stanowiących stacje robocze.

W uzasadnionych przypadkach, w szczególności gdy wymaga tego specyfika realizowanych zadań, dane mogą być przechowywane również na nośnikach mobilnych (dyski zewnętrzne, płyty CD/DVD/blue-ray, karty pamięci, pamięci USB). Użytkownicy nośników mobilnych są zobowiązani do stosowania wszystkich zasad dotyczących ochrony danych i bezpieczeństwa informacji obowiązujących w jednostce, w szczególności zaś uregulowań zawartych w punkcie *Wykorzystywanie nośników mobilnych*.

Jeżeli określone dane, a zwłaszcza dane osobowe nie będą już wykorzystywane, należy je usunąć z nośnika danych. Usunięcie danych powinno spełniać wymogi definicji tego pojęcia zawartej w przepisach o ochronie danych osobowych.

W przypadku zakończenia wykorzystywania danego nośnika danych, przed wycofaniem go z użytkowania należy trwale i skutecznie usunąć z niego dane.

W przypadku, gdy trwałe i skuteczne usunięcie danych nie jest możliwe, przed wycofaniem z eksploatacji nośnik ten powinien zostać uszkodzony w sposób uniemożliwiający odczytanie z niego danych.

Nośniki danych zawierające kopie zapasowe

Nośniki zawierające kopie zapasowe danych przechowuje się w bezpiecznych miejscach, zabezpieczone przed uszkodzeniem lub zniszczeniem oraz przed dostępem osób niepowołanych. Nośniki zawierające kopie danych, w skład których wchodzą dane osobowe przechowywane są z zachowaniem wszystkich uregulowań dotyczących bezpieczeństwa przy przetwarzaniu danych osobowych.

Nośniki danych zawierające kopie zapasowe danych powinny być przechowywane w innym pomieszczeniu niż to, w którym znajdują się nośniki zawierające podstawową, operacyjną kopię określonych danych.

Dostęp do nośników zawierających kopie zapasowe danych posiada wyłącznie administrator systemu informatycznego oraz ewentualnie osoba indywidualnie upoważniona przez Dyrektora.

Wykorzystywanie nośników mobilnych

Dane przechowywane na nośnikach mobilnych powinny być usuwane niezwłocznie po ustaniu powodów, dla których podjęto decyzję o wykorzystywaniu nośnika mobilnego.

Nośniki mobilne, zawierające chronione dane, w szczególności dane osobowe, w czasie, gdy nie są wykorzystywane powinny być przechowywane w bezpiecznym miejscu, w szczególności pod zamknięciem, aby zagwarantować niemożliwość dostępu do nich przez niepowołane osoby. Zaleca się stosowanie kryptograficznych środków ochrony wobec danych przechowywanych na nośnikach mobilnych.

Przechowywane nośniki mobilne zawierające chronione dane, powinny być oznakowane (opisane) w sposób umożliwiający jednoznaczna identyfikację kategorii danych na nich przechowywanych.

Osoby wykorzystujące nośniki mobilne są zobowiązane do dołożenia szczególnej staranności i szczególnej uwagi, aby nośniki ani dane na nich zapisane nie dostały się w ręce osób niepowołanych. W szczególności jeśli istnieją takie techniczne możliwości, dane przechowywane na nośnikach mobilnych powinny być zabezpieczane za pomocą środków ochrony kryptograficznej (szyfrowanie).

14. Usuwanie danych

Wszystkie chronione dane, w szczególności dane osobowe, w tym także kopie zapasowe danych powinny być usuwane niezwłocznie po ustaniu ich przydatności.

Przez usunięcie danych rozumie się zniszczenie danych lub taką ich modyfikację, która uniemożliwi odczytanie chronionych informacji. W szczególności w przypadku danych osobowych taką ich modyfikację, która uniemożliwi identyfikację osób, których dane dotyczą.

Niszczenie kopii zapasowych danych odbywa się komisyjnie. Komisję w tej sprawie powołuje Dyrekcja, Inspektor Ochrony Danych lub administrator systemu informatycznego. Z przeprowadzonego zniszczenia kopii komisja sporządza protokół. Protokoły dotyczące niszczenia kopii zapasowych dołącza się do dokumentacji dotyczącej ochrony danych.

15. Naprawy elementów systemów

Naprawa sprzętu i oprogramowania w systemach informatycznych wykorzystywanych w jednostce jest wykonywana wyłącznie przez osoby posiadające niezbędną wiedzę i doświadczenie w tego typu pracach.

Każdorazowo przy dopuszczeniu do prac naprawczych na sprzęcie lub oprogramowaniu osób trzecich należy podjąć działania mające na celu uniemożliwienie dostępu osób prowadzących naprawę do chronionych danych. W przypadku, gdy jest to niemożliwe a naprawa odbywa się w siedzibie jednostki, ta część prac, w trakcie której mogłoby dojść do dostępu do chronionych danych powinna być wykonywana pod nadzorem uprawnionego pracownika organizacji.

Jeżeli naprawa wymaga wyniesienia sprzętu poza siedzibę jednostki, ze wszystkich nośników danych, które będą wyniesione usuwa się dane podlegające ochronie, w szczególności dane osobowe.

Jeżeli usuniecie danych nie jest możliwe, sprzęt nie może być wyniesiony w ramach normalnych procedur naprawy elementów systemów. W takim przypadku indywidualną decyzję o wyrażeniu zgody na wyniesienie nośników danych, zawierających chronione dane, podejmuje Dyrektor, po zasięgnięciu opinii Inspektora Ochrony Danych. W każdym z tego typu przypadków należy rozważyć możliwość lub konieczność zastosowania dodatkowych środków zabezpieczających, w szczególności o charakterze formalnym.

16. Zabezpieczenia systemów przed złośliwym oprogramowaniem

W celu ochrony przed działalnością szkodliwego oprogramowania, w systemach informatycznych wykorzystywanych w organizacji stosuje się oprogramowanie antywirusowe.

Stacje robocze obejmuje się ochroną za pośrednictwem oprogramowania antywirusowego.

Konfiguracja oprogramowania antywirusowego powinna zapewniać skanowanie na bieżąco plików wprowadzanych do systemu, regularne, okresowe skanowanie całości systemu oraz każdorazowe skanowanie nośników zewnętrznych podłączanych do systemu.

Dla zapewnienia odpowiedniego poziomu ochrony stosuje się oprogramowanie antywirusowe, regularnie, na bieżąco aktualizowane w zakresie bazy wirusów.

Administrator systemu informatycznego jest odpowiedzialny za utrzymanie aktualności stosowanego oprogramowania antywirusowego oraz jego właściwą konfigurację.

Użytkownicy nie są uprawnieni do przerywania ani pomijania procesu skanowania nośników w poszukiwaniu wirusów i innego szkodliwego oprogramowania.

W przypadku, gdy użytkownik zauważy, że oprogramowanie antywirusowe wykryło obecność wirusa i wirus ten nie został usunięty, niezwłocznie informuje o tym fakcie administratora systemu informatycznego. Do czasu podjęcia działań przez administratora systemu informatycznego zabrania się korzystania z plików lub nośników, w których stwierdzono obecność wirusów, których nie udało się usunąć. Jeżeli wirus został znaleziony na nośniku mobilnym, nośnik taki należy jak najszybciej odłączyć od systemu i nie podłączać ponownie do czasu podjęcia działań przez administratora systemu informatycznego.

17. Zabezpieczenia systemów przed skutkami utraty zasilania

W celu ochrony przetwarzanych danych przed zniszczeniem spowodowanym zanikiem napięcia w sieci elektroenergetycznej w systemach informatycznych wykorzystywanych w jednostce, w miarę posiadanych możliwości ekonomicznych, stosuje się zabezpieczenia w postaci zasilaczy bezprzerwowych (UPS).

Ochronie zasilaczami bezprzerwowymi podlegają stacje robocze, na których przetwarzane są dane podlegające ochronie, w szczególności dane osobowe.

Zastosowane zasilacze bezprzerwowe powinny zapewniać czasy pracy systemu po zaniku napięcia w zasilającej system sieci elektroenergetycznej niezbędny dla bezpiecznego zakończenia wykonywanych operacji i zamknięcia systemu.

Zasilacze bezprzerwowe zastosowane przy stacjach roboczych powinny zapewnić im czas pracy bez dostępu zasilania z sieci elektroenergetycznej umożliwiający zapisanie i bezpieczne zakończenie pracy, wylogowanie z systemu i bezpieczne wyłączenie stacji roboczej.

Administrator systemu informatycznego jest zobowiązany do sprawdzania poprawności pracy zasilaczy bezprzerwowych.

Zaleca się prowadzenie okresowych kontroli możliwego czasu pracy na bateriach przez poszczególne zasilacze. Za prowadzenie tych kontroli odpowiedzialny jest administrator systemu informatycznego.

18. Dostęp do sieci publicznej

Administrator systemu informatycznego we współpracy z Inspektorem Ochrony Danych oraz Dyrekcją określa zasady podłączania lokalnej infrastruktury teleinformatycznej do sieci publicznej, w szczególności określa użytkowników, którzy uprawnieni są do korzystania z połączeń z siecią publiczną.

Administrator systemu informatycznego jest zobowiązany do zastosowania zabezpieczeń chroniących lokalną sieć teleinformatyczną przed niepowołanym dostępem z zewnątrz. W przypadku konfiguracji systemu umożliwiającej dostęp przez uprawnionych pracowników z zewnątrz stosuje się metody zapewniające poufność transmisji i ograniczające krąg użytkowników mających dostęp do sieci do zdefiniowanej i kontrolowanej przez administratora systemu informatycznego grupy użytkowników.

Administrator systemu informatycznego prowadzi aktualną ewidencję osób, które posiadają dostęp do lokalnej sieci komputerowej z sieci publicznej.

Konfiguracja zastosowanych narzędzi (sprzętowych i programowych) zastosowanych w celu ochrony systemów informatycznych w jednostce powinna być wykonana w taki sposób, by umożliwiać transmisję pomiędzy siecią lokalną a siecią publiczną w minimalnym, niezbędnym zakresie (zakres otwartych portów).

Przesyłanie danych podlegających ochronie, a zwłaszcza danych osobowych w sieci publicznej może się odbywać wyłącznie w postaci zaszyfrowanej.

a

Wykorzystanie do komunikacji w sieci lokalnej technologii bezprzewodowych (np. Wi-Fi) jest możliwe tylko w sytuacji http://www.seminarium-rodo.vulcan.edu.pl/ transmisji poprzez mechanizmy kryptograficzne (szyfrowanie). Zastosowanie w systemie informatycznym jednostki technologii bezprzewodowych wymaga zgody Dyrektora i może być wdrażane wyłącznie pod nadzorem administratora systemu informatycznego.

Ze względu na charakter działalności jednostki, w szczególności fakt, iż istotną grupą użytkowników systemów informatycznych (w tym infrastruktury i dostępu do Internetu) są osoby niepełnoletnie, powinno zostać zastosowane oprogramowanie

służące analizie i filtracji treści przesyłanych do i z sieci publicznej (w szczególności w celu ograniczenia możliwości pobierania i wyświetlania treści pornograficznych lub innych niezgodnych z obowiązującym prawem).

Administrator systemu informatycznego jest odpowiedzialny za monitorowanie wdrożonych zabezpieczeń, w tym do regularnego śledzenia zapisów w logach systemowych.

19. Komputery przenośne, praca poza siedzibą

Osoby użytkujące w swojej pracy komputery przenośne zobowiązane są do zachowania szczególnej ostrożności w trakcie wykorzystywania go, zwłaszcza poza siedzibą Windbud Sp. z o.o..

Szczególna ostrożność, o której mowa powyżej, powinna być zachowana w szczególności w zakresie:

- transportu komputera, kiedy należy zwracać szczególną uwagę na zagrożenie zabrania komputera bądź nośników danych przez osobę nieuprawnioną, uszkodzenia mechanicznego komputera, w wyniku którego może nastąpić uszkodzenie bądź utrata danych lub magnetycznego, w wyniku którego może nastąpić utrata danych,
- przechowywania komputera, kiedy należy zwracać szczególną uwagę na zagrożenie zabrania komputera bądź nośników danych przez osobę nieuprawnioną, uszkodzenia mechanicznego lub magnetycznego, w wyniku którego może nastąpić uszkodzenie lub utrata danych,
- użytkowania komputera, kiedy należy zwracać szczególną uwagę na zagrożenie podejrzenia danych podlegających ochronie na ekranie komputera lub włamania do systemu za pomocą technologii bezprzewodowych.

Administrator systemu informatycznego jest zobowiązany przed przekazaniem komputera przenośnego do użytkowania, zastosować na nim środki zabezpieczające, dobrane adekwatnie do sposobu użytkowania tego komputera, kategorii danych, które będą na nim przetwarzane oraz potencjalnych zagrożeń.

W trakcie doboru zabezpieczeń komputera przenośnego administrator systemu informatycznego jest zobowiązany rozważyć do zastosowania między innymi:

- zabezpieczenie dostępu do komputera hasłem na poziomie sprzętowym,
- zabezpieczenie dostępu do systemu operacyjnego za pomocą mechanizmów uwierzytelniania,

- zastosowanie kryptograficznych środków ochrony danych przechowywanych na nośnikach danych wchodzących w skład komputera przenośnego,
- zastosowanie narzędzi programowych ograniczających dostęp do chronionych danych.

Osoba użytkująca komputer przenośny jest zobowiązana do zachowania szczególnej ostrożności podczas podłączania komputera do sieci publicznej.

Użytkownik komputera przenośnego nie jest uprawniony do udostępniania go, w dowolnym celu, do używania przez osoby trzecie.

Za wszelkie działania podejmowane z użyciem komputera przenośnego wykorzystywanego poza obszarem siedziby jednostki oraz wszelkie konsekwencje z tego wynikające odpowiedzialność ponosi użytkownik tego komputera.

W przypadku istnienia konieczności wykorzystania do pracy poza siedzibą jednostki sprzętu, innego niż przypisany użytkownikowi komputer przenośny, będącego w posiadaniu organizacji każdorazowo pracownik jest zobowiązany uzyskać zgodę swojego bezpośredniego przełożonego albo Dyrekcji.

Zabrania się samowolnego wynoszenia przez pracowników sprzętu poza siedzibę jednostki.

20. Wykorzystywanie sprzętu prywatnego pracowników

Systemy informatyczne funkcjonujące w jednostce mogą być wykorzystywane przez pracowników wyłącznie do realizacji zadań wynikających z zakresów ich obowiązków służbowych.

Jeżeli dla celów właściwej realizacji swoich obowiązków pracownik chce wykorzystać posiadany przez siebie prywatnie sprzęt, może się to odbywać na następujących zasadach:

- prywatne nośniki danych mogą być wykorzystywane wyłącznie po poddaniu ich, przy każdorazowym podłączeniu do systemu, kontroli antywirusowej za pomocą oprogramowania antywirusowego. Jeżeli na tych nośnikach danych zapisane zostają dane podlegające ochronie w jednostce, wówczas przed wyniesieniem ich poza siedzibę użytkownik zobowiązany jest bezwzględnie usunąć z nich te dane (wymogi w zakresie usuwania danych zawarte w niniejszej Instrukcji stosuje się odpowiednio),
- prywatny sprzęt komputerowy pracownika może być wykorzystywany przez niego swobodnie w sytuacji, gdy nie jest podłączany do infrastruktury teleinformatycznej jednostki. W przypadku chęci podłączenia sprzętu do infrastruktury teleinformatycznej pracownik obowiązany jest zgłosić ten fakt administratorowi systemu informatycznego i uzyskać jego zgodę.

Dyrektor w każdej chwili może zarządzić zmianę obowiązujących zasad wykorzystywania przez pracowników prywatnego sprzętu. W związku z tym zaleca się, by pracownik chcący skorzystać ze swojego prywatnego sprzętu każdorazowo zasięgał opinii administratora systemu informatycznego, Inspektora Ochrony Danych lub swojego bezpośredniego przełożonego.

21. Przeglądy i konserwacje

Dla utrzymania jak najwyższego poziomu niezawodności funkcjonowania systemów informatycznych funkcjonujących w jednostce systemy te poddaje się regularnym przeglądom i konserwacji.

Za organizację przeglądów i konserwacji systemów odpowiedzialny jest administrator systemu informatycznego.

Administrator systemu informatycznego może przeprowadzać przeglądy i konserwacje osobiście lub przy pomocy wyspecjalizowanych firm zewnętrznych. Zaleca się, by okresowo korzystać z zewnętrznych konsultantów przy prowadzeniu przeglądów systemów. Przy realizowaniu zadań związanych z przeglądami i konserwacją systemów przez zewnętrznych konsultantów obowiązują analogiczne zasady bezpieczeństwa, jak przy naprawie elementów systemu (opisane w części *Naprawa elementów systemu*).

Przeprowadzenie przeglądu oraz wnioski z niego płynące powinny być dokumentowane i dołączane do dokumentacji związanej z systemami informatycznymi wykorzystywanymi w organizacji.

Postanowienia końcowe

Wszystkich użytkowników systemów informatycznych obowiązują powszechnie obowiązujące przepisy prawa polskiego, w szczególności 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) (Dz. Urz. UE, L 119 z 4.05.2016), oraz związanych z nim polskich i europejskich aktów normatywnych.

Windbud Sp. z o.o.

POLITYKA ZARZĄDZANIA INCYDENTAMI

Zarządzanie incydentami związanymi z bezpieczeństwem informacji

Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji i słabości

Aby zapewnić skuteczność funkcjonowania systemu bezpieczeństwa informacji w jednostce wprowadza się zasady zgłaszania zdarzeń związanych z bezpieczeństwem informacji oraz słabości systemów.

Wszyscy pracownicy są zobowiązani do postępowania zgodnie z uregulowaniami niniejszego dokumentu.

Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji

W przypadku zauważenia jakiegokolwiek zdarzenia mogącego wpłynąć negatywnie na bezpieczeństwo informacji, w tym w szczególności bezpieczeństwo danych osobowych, każdy pracownik bądź współpracownik jest zobowiązany podjąć działania opisane w niniejszym dokumencie, w szczególności zgłosić ten fakt odpowiednim osobom.

Kwalifikacji zdarzenia jako mogącego wpłynąć na bezpieczeństwo informacji (incydentu) dokonuje osoba obserwująca to zdarzenie. Za tego typu zdarzenia uważa się w szczególności:

- utratę usługi, urządzenia lub funkcjonalności,
- przeciążenie lub niepoprawne działanie systemu,
- błędy ludzkie wpływające na bezpieczeństwo,
- niezgodność działania bądź postępowania z politykami lub zaleceniami,
- naruszenia ustaleń związanych z bezpieczeństwem fizycznym, w tym nieuprawniony dostęp do danych lub obszaru przetwarzania, kradzież sprzętu bądź nośników danych,

- niekontrolowane zmiany systemu lub zabezpieczeń, w tym wszelkie próby naruszenia poufności, integralności i rozliczalności systemu bądź danych,
- naruszenia dostępu,
- zdarzenia losowe.

Procedura zgłaszania incydentów związanych z bezpieczeństwem danych

W przypadku zauważenia zdarzenia wpływającego bądź mogącego mieć wpływ na bezpieczeństwo informacji osoba, która powzięła taką informację powinna:

- zawiadomić o tym fakcie Inspektora Ochrony Danych, swojego bezpośredniego przełożonego lub dyrekcję. Zawiadomienie powinno nastąpić tak szybko, jak jest to możliwe,
- zapamiętać lub zanotować wszystkie ważne szczegóły dotyczące zdarzenia (np. typ niezgodności lub naruszenia, błąd działania, wiadomość z ekranu, dziwne zachowanie itp.),
- nie podejmować żadnych dalszych działań do czasu interwencji wyznaczonych pracowników, zwłaszcza wówczas, gdy dalsze działania mogłyby pogłębić ujawnione problemy lub zatrzeć ślady związane ze zidentyfikowanym wcześniej naruszeniem,
- jeżeli naruszenie spowodowało sytuację, w której istnieje zagrożenie dostępu do chronionych danych, a w szczególności danych osobowych, przez osoby nieuprawnione, wówczas niezależnie od oczekiwania na interwencję wyznaczonych pracowników każdy pracownik jest zobowiązany do zabezpieczenia danych w celu uniemożliwienia dostępu do nich przez niepowołane osoby.

Zawiadomienie powinno zostać przeprowadzone w formie, która umożliwia najszybsze przekazanie informacji. Jeżeli jednak naruszenie dotyczy zagadnień ochrony danych osobowych informacja o naruszeniu powinna być dostarczona również w formie pisemnej.

Odpowiedzialność za niezgłoszenie znanego incydentu

Niezgłaszanie zauważonych naruszeń będzie traktowane jako naruszenie systemu bezpieczeństwa i może podlegać odpowiedzialności dyscyplinarnej bądź karnej.

Zgłaszanie słabości systemu bezpieczeństwa

W przypadku, gdy użytkownik zaobserwował lub podejrzewa istnienie słabości w systemie bezpieczeństwa jest zobowiązany zgłosić ten fakt administratorowi systemu informatycznego lub swojemu bezpośredniemu przełożonemu.

Jednocześnie użytkownicy nie są uprawnieni do testowania zabezpieczeń systemu. W związku z tym niedopuszczalne jest dowodzenie istnienia podejrzewanej słabości, a obowiązek dotyczy jedynie zgłoszenia podejrzenia jej występowania.

Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami

Odpowiedzialność i procedury

Osoby zarządzające dokładają wszelkich starań, by reakcja na incydenty związane z bezpieczeństwem informacji przebiegała w sposób szybki, skuteczny i uporządkowany.

Na chwilę ogłoszenia niniejszej Polityki bezpieczeństwa nie ustanawia się specjalnych, dedykowanych procedur do obsługi poszczególnych typów incydentów, przy czym dopuszcza się możliwość ich ustanawiania w ramach rozwoju systemu zarządzania bezpieczeństwem informacji w przyszłości.

W przypadku pojawienia się incydentu związanego z bezpieczeństwem informacji podejmuje się właściwe działania, uwzględniając:

- analizę i identyfikację przyczyny incydentu,
- ograniczanie zasięgu naruszenia bezpieczeństwa,
- planowanie i wdrażanie działań naprawczych w celu uniknięcia powtórnego wystąpienia incydentu,

- komunikację z podmiotami związanymi z incydentem i zaangażowanymi w jego usunięcie,
- dokumentację prowadzonych działań,
- gromadzenie ewentualnych dowodów,
- utrzymanie ciągłości działania.

Incydenty związane z przetwarzaniem danych osobowych

Jeżeli zaistniały incydent związany jest z przetwarzaniem danych osobowych dokonuje się kwalifikacji incydentu, jego analizy pod kątem wystąpienia naruszenia ochrony oraz podejmuje wymagane prawem (w szczególności przepisami RODO) działania, a także przeprowadza się postępowanie wyjaśniające.

Prace związane z incydentami oraz naruszeniami koordynuje Inspektor Ochrony Danych.

Kwalifikacja incydentu

Niezwłocznie po wykryciu incydentu i zebraniu niezbędnych informacji dokonuje się oceny, czy incydent stanowi naruszenie w rozumieniu przepisów RODO.

Do prowadzenia oceny, o której mowa powyżej stosuje się *Kartę oceny incydentu*, stanowiącą Załącznik nr 1 do niniejszej Polityki.

Jeżeli incydent zostaje zakwalifikowany jako naruszenie dokonuje się oceny naruszenia. W przypadku, kiedy incydent nie jest naruszeniem przechodzi się do postępowania wyjaśniającego.

Kwalifikacja incydentu

Niezwłocznie po stwierdzeniu, że naruszenie jest incydentem dokonuje się analizy tego naruszenia pod kątem ewentualnej konieczności wykonania obowiązków wynikających z przepisów art. 33 i 34 RODO (zgłoszenie naruszenia organowi nadzorczemu oraz poinformowanie o naruszeniu podmiotów danych).

Do prowadzenia analizy naruszenia, o której mowa powyżej stosuje się *Kartę oceny naruszenia*, stanowiącą Załącznik nr …… do niniejszej Polityki.

Każde stwierdzone naruszenie podlega wpisowi do prowadzonego rejestru naruszeń. Wzór Rejestru naruszeń stanowi Załącznik nr 2 do niniejszej Polityki.

Postępowanie wyjaśniające

Wobec naruszeń oraz incydentów prowadzi się postępowanie wyjaśniające. Dyrekcja wyznacza osobę lub osoby odpowiedzialne za prowadzenie postępowań wyjaśniających. Jeżeli Dyrekcja nie wyznaczy takiej osoby, domyślnie odpowiedzialnym za prowadzenie postępowań wyjaśniających jest Inspektor Ochrony Danych. W przypadku drobnych incydentów Dyrekcja lub Inspektor Ochrony Danych mogą podjąć decyzję o odstąpieniu od prowadzenia postępowania wyjaśniającego. Postępowanie wyjaśniające wobec naruszeń prowadzi się w każdym przypadku.

W przypadku otrzymania informacji o incydencie lub naruszeniu osoba odpowiedzialna za prowadzenie postępowań wyjaśniających:

- udaje się na miejsce wystąpienia incydentu,
- dokonuje przeglądu i oceny sytuacji zastanej, ze szczególnym uwzględnieniem stanu urządzeń i pomieszczeń w momencie przybycia,
- odbiera relację dotyczącą zdarzeń związanych z incydentem od osoby zgłaszającej incydent, a także jeśli jest taka konieczność od innych osób, których wiedza może być pomocna przy ustalaniu okoliczności incydentu,
- wydaje polecenia i podejmuje decyzje w zakresie prowadzenia dalszych działań. Wszyscy pracownicy, których działania mogą mieć związek z incydentem bądź jego usuwaniem są zobowiązani do bezwzględnej realizacji tych poleceń,
- jeżeli naruszenie jest wynikiem niezastosowania się przez pracowników bądź współpracowników do obowiązujących przepisów prawa lub uregulowań wewnętrznych dotyczących bezpieczeństwa informacji lub ochrony danych osobowych, osoba prowadząca postępowanie wyjaśniające wnioskuje do Dyrekcji o wyciągnięcie stosownych konsekwencji. Do wniosku dołącza się zgromadzony w wyniku postępowania wyjaśniającego materiał dowodowy,
- w zależności od sytuacji i potrzeb z postępowania wyjaśniającego może być sporządzony protokół. Jeśli naruszenie dotyczyło ochrony bądź przetwarzania

danych osobowych, osoba prowadząca postępowanie wyjaśniające jest zobowiązana do sporządzenia protokołu z prowadzonego postępowania i po jego zakończeniu przekazania go Dyrekcji. Protokół te powinien zawierać co najmniej:

- informacje o czasie – prawdopodobnym zaistnienia zdarzenia, zgłoszenia incydentu oraz przybycia na miejsce osoby prowadzącej postępowanie wyjaśniające,
- informacje o osobach związanych z incydentem, w szczególności o zgłaszającym oraz prowadzącym postępowanie,
- opis sytuacji zastanej po przybyciu na miejsce wystąpienia incydentu, w tym opis stanu systemów, urządzeń i pomieszczeń,
- opis podjętych działań,
- opis efektów uzyskanych w wyniku podjętych działań,
- opis przyczyny lub prawdopodobnej przyczyny zaistnienia incydentu,
- ewentualne wnioski ogólne, mające na celu zmniejszenie prawdopodobieństwa wystąpienia podobnego incydentu w przyszłości.

Wyciąganie wniosków z incydentów związanych z bezpieczeństwem informacji

Regularnie prowadzi się analizę występujących incydentów i naruszeń oraz wyciąga wnioski z tej analizy. W uzasadnionych przypadkach wnioski z analizy, o której mowa powyżej, stanowią podstawię do wnioskowania zmian w obowiązującej Polityce bezpieczeństwa.

Gromadzenie materiału dowodowego

W przypadku, gdy naruszenie może powodować kroki prawne (natury dyscyplinarnej, cywilnoprawnej lub karnej), w szczególności, gdy naruszenie dotyczy ochrony danych osobowych, w ramach czynności związanych z obsługą incydentu powinien być gromadzony, zachowywany, a na właściwym etapie przedstawiany materiał dowodowy.

Załącznik nr 1

KARTA OCENY INCYDENTU

POD KĄTEM WYSTĄPIENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

DANE ADMINISTRATORA DANYCH			
Nazwa			
Adres			
Imię i nazwisko Inspektora Ochrony Danych			
OKOLICZNOŚCI STWIERDZENIA INCYDENTU			
Data i godzina stwierdzenia incydentu			
Osoba, która stwierdziła/zaobserwowała incydent			
OPIS INCYDENTU			
PODSTAWOWA ANALIZA INCYDENTU			
Czy w wyniku incydentu doszło zniszczenia lub utracenia danych osobowych?	TAK	NIE	
Czy istnieje możliwa do odtworzenia kopia zniszczonych lub utraconych danych?	NIE	TAK	
Czy w wyniku incydentu doszło do nieuprawnionego lub niekontrolowanego zmodyfikowania treści danych osobowych?	TAK	NIE	
Czy w wyniku incydentu nastąpiło nieuprawnione ujawnienie danych osobowych?	TAK	NIE	Nie można jednoznacznie określić
Czy w wyniku incydentu mogło dość dojść do ujawnienia danych osobowych?	NIE		TAK
Czy w wyniku incydentu doszło do dostępu do danych przez osobę nieuprawnioną? (w tym pobrania danych, zabrania dokumentów itp.)	TAK	NIE	Nie można jednoznacznie określić
Czy w wyniku incydentu mogło dość dojść do dostępu do danych przez osobę nieuprawnioną?	NIE		TAK
KWALIFIKACJA INCYDENTU			
Czy incydent jest naruszeniem?		TAK / NIE*	
Uzasadnienie:			

……..
data

podpis osoby przeprowadzającej analiz

……

……..

* - niepotrzebne skreślić.

Załącznik nr 2

KARTA OCENY NARUSZENIA

POD KĄTEM REALIZACJI OBOWIĄZKÓW WYNIKAJĄCYCH Z ART. 33 I 34 RODO

DANE ADMINISTRATORA DANYCH	
Nazwa	
Adres	
Imię i nazwisko Inspektora Ochrony Danych	
OKOLICZNOŚCI STWIERDZENIA NARUSZENIA	
Data i godzina stwierdzenia naruszenia?	
Osoba, która stwierdziła naruszenie?	
W jaki sposób administrator danych dowiedział się o naruszeniu?	
OPIS NARUSZENIA	
CECHY NARUSZENIA	
Jakiej kategorii osób dane zostały dotknięte naruszeniem?	
Jaka jest istota naruszenia? (ujawnienie, zniszczenie, modyfikacja danych)	
Jakiej liczby osób dotyczy naruszenie?	
Jakiego zakresu danych o poszczególnych osobach dotyczy naruszenie?	
Czy naruszenie obejmuje dane szczególnie chronione (tzw. dane wrażliwe)?	
Czy naruszenie obejmuje dane niebędące danymi wrażliwymi, ale o szczególnym znaczeniu dla osób, których te dane dotyczą?	

Jak trudno jest pozyskać dane, które zostały ujawnione? (dotyczy sytuacji ujawnienia danych osobom nieuprawnionym)	
Jak trudno jest odtworzyć dane, które zostały utracone lub zmodyfikowane? (dotyczy sytuacji zniszczenia danych lub ich nieuprawnionej modyfikacji)	
ANALIZA POTENCJALNYCH SKUTKÓW	
W jakim – także nielegalnym – celu można wykorzystać dane wchodząc w ich posiadanie? (dotyczy sytuacji ujawnienia danych osobom nieuprawnionym)	
Jakie konsekwencje– w najbardziej pesymistycznym scenariuszu – mogą spotkać osoby, których dane dotyczą w związku z naruszeniem? Czy konsekwencje te są odwracalne?	
Czy ujawnione dane można wykorzystać do kradzieży tożsamości?	
Czy ujawnione dane można wykorzystać do zaciągnięcia zobowiązań, w szczególności finansowych?	
Czy za pomocą ujawnionych danych można ośmieszyć osobę lub w inny sposób naruszyć jej dobra osobiste?	
Czy za pomocą ujawnionych danych można naruszyć dobra osobiste osób trzecich? Co to są za osoby?	
WPŁYW	
Jakie prawa lub wolności osób, których dane dotyczą lub innych osób mogą zostać naruszone w wyniku analizowanego naruszenia?	
AKTUALNY STAN	
Czy naruszenie zostało usunięte?	
Jeżeli naruszenie nie zostało jeszcze usunięte, to jaki jest szacowany termin usunięcia naruszenia?	

Jakie środki i działania podjęto po stwierdzeniu naruszenia?	
INNE INFORMACJE	
WNIOSKI Z ANALIZY	
Czy jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych? (art. 33 ust. 1 RODO)	TAK / NIE*
Uzasadnienie:	
Czy naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych? (art. 34 ust. 1 RODO)	TAK / NIE*
Czy dotychczas zastosowano lub planuje się zastosować środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą w związku z tym naruszeniem?	TAK / NIE*
Czy naruszenie podlega obowiązkowi zawiadomienia osób, których dane dotyczą, zgodnie z przepisami art. 34 RODO?	TAK / NIE*
Uzasadnienie:	

…….…….. ……

data ……..

podpis osoby przeprowadzającej analiz

* - niepotrzebne skreślić.

Windbud Sp. z o.o.

ZASADY PROWADZENIA ANALIZY RYZYKA

Proces zarządzania ryzykiem prowadzony w szkole jest punktem wyjścia do zapewnienie bezpieczeństwa przetwarzania danych zarówno w systemach informatycznych jak i tych przetwarzanych w wersji papierowej.

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne w celu:

- aby przetwarzanie odbywało się zgodnie z RODO,

- aby móc wykazać, że przetwarzanie odbywa się zgodnie z RODO.

I. Podstawowe pojęcia

Aktywa – jest to wszystko, co ma wartość dla organizacji (administratora danych lub podmiotu przetwarzającego), np. dane osobowe.

Właściciel aktywów – jest to osoba odpowiedzialna w danym podmiocie za konkretny proces przetwarzania danych i mająca prawo do podejmowania w tym zakresie decyzji, np. dyrektor departamentu, kierownik określonej komórki w organizacji.

Kontekst – są to wszystkie informacje wiążące się z działaniem organizacji, m.in. informacje dotyczące środowiska prawnego, społecznego, politycznego, finansowego czy też technologicznego, np. przepisy dotyczące ochrony danych osobowych.

Zagrożenie – jest to źródło potencjalnej szkody, np. zagrożenie naruszenia integralności danych.

Zabezpieczenie – jest to środek, którego celem jest zmniejszenie ryzyka poprzez obniżenie prawdopodobieństwa zrealizowania zagrożenia (czyli wykorzystania istniejącej podatności) lub też minimalizację potencjalnych strat związanych ze zrealizowanym zagrożeniem, np. program antywirusowy, drzwi antywłamaniowe, stosowanie procedury bezpieczeństwa.

Podatność – jest to słabość, która może być wykorzystana przez zagrożenie, powodując niekorzystne skutki, np. luka w systemie informatycznym. Słabość aktywa lub zabezpieczenia, która może być wykorzystana do urzeczywistnienia się zagrożenia.

Ryzyko – wpływ niepewności na cele. W przypadku ryzyka naruszenia praw i wolności osób, których dane dotyczą, celem będzie ochrona tych praw i wolności.

Identyfikowanie ryzyka – jest to czynność polegająca na określeniu, co może się zdarzyć (kiedy, gdzie, jak i dlaczego) i spowodować stratę.

Szacowanie ryzyka – całościowy proces identyfikacji ryzyka, analizy ryzyka oraz oceny ryzyka (definicja przyjęta zgodnie z normą PN-ISO/IEC 25005:2011)

Szczątkowe ryzyko – ryzyko pozostające po zastosowaniu działań określonych w postępowaniu z ryzykiem

Zarządzanie ryzykiem – skoordynowane działania dotyczące kierowania i nadzorowania szkoły w odniesieniu do ryzyka

II. Ustalenie kontekstu

Zgodnie z art. 24 ust. 1 i art. 32 ust. 1 RODO, w procesie szacowania ryzyka należy uwzględniać wiele czynników, m.in. wagi zagrożeń, wynikającej z rodzaju skutku urzeczywistnienia się zagrożeń, np. uszczerbku fizycznego, dyskryminacji itp. Proces, w którym należy dokonać analizy tych czynników nazywany jest ustanowieniem kontekstu, w ramach którego należy dokonać inwentaryzacji potencjalnych zdarzeń mogących być źródłem ryzyka oraz określić kryteria oceny poziomu ryzyka i kryteria jego akceptacji.

Kontekst wewnętrzny

Lp.	Czynniki wewnętrzne	Oczekiwania	Zagrożenia	Rozwiązania
1	Kadra	Wykwalifikowana, świadoma zagrożeń kadra	Umyślne lub nieumyślne ujawienie informacji przez pracownika	Budowanie świadomości i kwalifikacji pracowników przez szkolenia
2	Uczniowie			
3	Systemy Informatyczne i infrastruktura			
4	Prowadzona dokumentacja			

Kontekst zewnętrzny

Lp.	Czynniki zewnętrzne	Oczekiwania	Zagrożenia	Rozwiązania
1	Przepisy prawa	Zgodność z przepisami prawa, przejrzystość stosowania przepisów	Nieprzestrzeganie przepisów i narażenie się na negatywne konsekwencje	Monitorowanie wymagań prawnych, konsultowanie, uczestnictwo w szkoleniach,
2	Rodzice			
3	Dostawcy usług			
4	Instytucje nadzorujące i współpracujące			

III. Szacowanie ryzyka

KROK 1. INWENTARYZACJA AKTYWÓW

Na tym etapie określamy listę aktywów informacyjnych, które należy brać pod uwagę w trakcie procesu analizy ryzyka. W szkole możemy określić kilka rodzajów aktywów:

sprzęt – wszelkie urządzenia fizyczne w organizacji tj.: urządzenia przenośne, stacjonarne, peryferyjne, nośniki danych;

oprogramowanie – wszelkie programy uczestniczące w operacjach przetwarzania danych tj.: systemy operacyjne, aplikacje biznesowe, oprogramowania usługowe, utrzymaniowe lub administracyjne;

sieć – wszystkie urządzenia telekomunikacyjne używane do połączenia wielu fizycznie oddalonych komputerów lub elementów systemu informacyjnego, tj.: media i usługi wspierające, przekaźniki aktywne lub pasywne, interfejsy komunikacyjne;

personel – wszystkie grupy osób zaangażowane w przetwarzanie danych tj.: decydenci, użytkownicy, personel eksploatacji/utrzymania, twórcy oprogramowania;

siedziba – wszelkie lokalizacje wykorzystywane do przetwarzania danych oraz środki fizyczne potrzebne do ich funkcjonowania tj. siedziba, strefy bezpieczeństwa, usługi komunalne i techniczne;

organizacja – wszystkie struktury ludzkie przypisane do przetwarzania danych oraz procedury sterujące tymi strukturami, tj.: struktura organizacji szkoły, podwykonawcy (procesorzy), dostawcy, producenci;

dokumenty w formie papierowej – dane przetwarzanie w wersji papierowej.

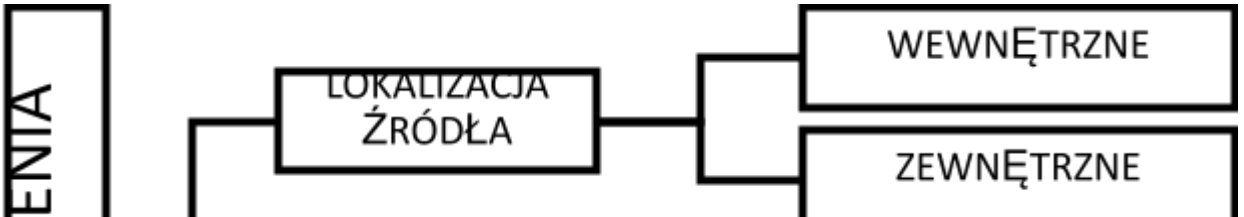
formaty plików w postaci elektronicznej – dane nieustrukturyzowane przetwarzanie w wersji elektronicznej

KROK 2. IDENTYFIKACJA ZAGROŻEŃ

Zidentyfikowane podstawowych zagrożeń występujących w kontekście procesu przetwarzania danych i informacji, w tym danych osobowych. Poniższą listę należy traktować jako punkt wyjścia w analizie i ocenie ryzyka związanego z przetwarzaniem danych. Nie stanowi ona katalogu zamkniętego i może podlegać modyfikacjom i uzupełnieniom w trakcie każdorazowej identyfikacji i oceny ryzyka dla całej organizacji.

Rodzaj zagrożenia	Zagrożenie
Zniszczenia fizyczne	Pożar Zalanie Zniszczenie urządzeń lub nośników Pył, korozja
Zjawiska naturalne	Powódź Zjawiska pogodowe
Utrata usług	Utrata dostaw prądu Awaria urządzenia telekomunikacyjnego
Naruszenie bezpieczeństwa informacji	Kradzież nośników lub dokumentów Kradzież urządzenia Odtworzenie z wyrzuconych urządzeń Dane z niewiarygodnych źródeł Szpiegostwo, podsłuch
Awarie techniczne	Awaria urządzenia Przeciążenie systemu informacyjnego Niewłaściwe funkcjonowanie oprogramowania
Nieautoryzowane działania	Nieautoryzowane użycie urządzeń Nieuprawnione kopiowanie oprogramowania Zniekształcenie danych Nielegalne przetwarzanie danych
Naruszenie bezpieczeństwa funkcji	Błąd użytkowania Naruszenie praw Fałszowanie praw Naruszenie dostępności personelu

Zagrożenia ze względu na źródło i przyczynę



KROK 3. IDENTYFIKACJA PODATNOŚCI

Dla każdego zagrożenia zidentyfikowanego w ramach grupy aktywów (zasobów) należy określić podatność.

Rodzaj aktywów	Podatność
Sprzęt	Brak staranności przy pozbywaniu się nośników Niekontrolowane kopiowanie Wrażliwość na zmiany temperatury Niewłaściwe zabezpieczenie okablowania Brak kopii zapasowych Wrażliwość na zmiany napięcia
Oprogramowanie	Brak mechanizmów identyfikacji i uwierzytelniania, takich jak uwierzytelnianie użytkownika Złe zarządzanie hasłami Błędne przypisanie praw dostępu Brak kopii zapasowych Skomplikowany interfejs użytkownika Wady oprogramowania Niedojrzałe lub nowe oprogramowanie Brak dokumentacji lub niejasny, niekompletny opis działania oprogramowania
Sieć	Brak dowodu wysłania lub odebrania wiadomości Niezabezpieczone linie telekomunikacyjne Złe łączenie kabli Pojedynczy punkt uszkodzenia Brak identyfikacji i uwierzytelnienia nadawcy i odbiorcy Przesyłanie hasła w jawnej postaci Nieodpowiednie zarządzanie siecią Niezabezpieczone połączenia z siecią publiczną
Personel	Nieobecność personelu Niewystarczające szkolenie z bezpieczeństwa Brak świadomości w zakresie bezpieczeństwa Niepoprawne użycie oprogramowania lub sprzętu Praca personelu zewnętrznego lub sprzątającego bez nadzoru Brak polityki w zakresie poprawnego użytkowania środków telekomunikacyjnych i komunikatorów
Siedziba	Brak fizycznej ochrony budynków, drzwi i okien

	Nieodpowiednie lub niestaranne użytkowanie fizycznej kontroli dostępu do budynków i pomieszczeń Lokalizacja na obszarach zagrożonych powodzią Niestabilna sieć elektryczna
Organizacja	Brak lub niewystarczające zapisy (odnoszące się do bezpieczeństwa) w umowach z pracownikami i stronami trzecimi Brak regularnych audytów (nadzór) Brak procedur identyfikowania i szacowania ryzyka Brak lub niewystarczająca umowa o poziomie usług Brak właściwego przypisania zakresów odpowiedzialności związanych z bezpieczeństwem informacji Brak procedur przetwarzania informacji Brak formalnej polityki korzystania z komputerów przenośnych Brak lub niewystarczająca polityka „czystego biurka i czystego ekranu” Brak procedur raportowania o słabościach bezpieczeństwa

KROK 4. SZACOWANIE POZIOMU RYZYKA

Zaproponowana metodologia szacowania ryzyka została oparta o normy ISO i wytyczne GIODO.

Do oszacowania poziomu ryzyka, dla zdarzenia musimy ocenić wpływ na reputację szkoły oraz wpływ finansowy, czyli ewentualne kary, które może ponieść szkoła. Następnie dla zdarzenia oceniamy prawdopodobieństwo:

- zniszczenia fizycznego i naturalnego,

- utraty podstawowych usług i awarie techniczne,

- naruszeń bezpieczeństwa informacji,

- nieautoryzowanych działań i naruszeń bezpieczeństwa funkcji, w tym zagrożeń osobowych zewnętrznych.

1. Ocena prawdopodobieństwa wystąpienia zagrożenia

Wartość PR	Prawdopodobieństwo	Opis
5	prawie pewne	Istnieją przesłanki, by ocenić, że zagrożenie zmaterializuje się w najbliższej przyszłości

		/Zdarzenie występuje co najmniej raz na pół roku/
4	wysoce prawdopodobne	Istnieją przesłanki, by ocenić, że zagrożenie się zmaterializuje /Zdarzenie występowało co najmniej raz w ciągu roku/
3	możliwe	Wystąpienie zagrożenia jest realne /Zdarzenie występowało co najmniej raz w ciągu 3 lat/
2	mało prawdopodobne	Wystąpienie zagrożenia jest mało prawdopodobne /Zdarzenie zdarzało się w przeszłości (w ciągu ostatnich 5 lat)/
1	bardzo rzadkie	Możliwość wystąpienia zagrożenia jest znikoma /Zdarzenie nie występuje w przeszłości/

2. Stosowane zabezpieczenia

Zabezpieczenia techniczne i fizyczne

Wartość Z.TECH.	Poziom	Opis
6	wysoki	Do ochrony wykorzystywane są nowoczesne rozwiązania, posiadające certyfikację bezpieczeństwa
4,5	średni	Ochrona z zastosowaniem rozwiązań technicznych i fizycznych, regularnie audytowane i dostosowywane do zmieniającej się sytuacji
3	niski	Stosowanie tylko podstawowych rozwiązań technicznych i fizycznych, rzadko albo wcale nie audytowane
1,5	brak	Brak zabezpieczeń technicznych i fizycznych

Zabezpieczenia organizacyjne (w tym personale)

Wartość Z.ORG.	Skutek	Opis
6	wysoki	Zabezpieczenia organizacyjne są wdrożone, skuteczne i podlegają okresowym przeglądom
4,5	średni	Objęto ochroną organizacyjną, personalną i prawną, finansową lub ubezpieczeniową
3	niski	Podstawowa ochrona organizacyjna, personalna i prawna
1,5	brak	Brak ochrony organizacyjnej, prawnej, finansowej lub ubezpieczeniowej

3. Analiza i ocena skutków wystąpienia zagrożeń

Oddziaływanie finansowe

Wartość OF	Skutek	Opis
3	wysoki	znaczny wpływ na finanse, możliwe wysokie kary finansowe
2	umiarkowane	umiarkowany wpływ na finanse, możliwe kary finansowe
1	brak wpływu	brak wpływu na finanse

Wpływ na reputację

Wartość OR	Skutek	Opis
5	bardzo wysoki	negatywne opinie w mediach krajowych, możliwe konsekwencje pracownicze
4	wysoki	negatywne opinie w mediach lokalnych, możliwe konsekwencje pracownicze
3	średni	oddziaływanie lokalne, negatywne opinie w środowisku, bez udziału mediów
2	niski	negatywne opinie wśród części rodziców, o ograniczonym zasięgu, bez udziału mediów
1	znikomy	brak wpływu na reputację szkoły

4. Ocena poziomu ryzyka

WARIANT 1

Poziom ryzyka wyrażony jest w kategoriach kombinacji skutków oraz ich prawdopodobieństw., pomniejszony o poziom stosowanych zabezpieczeń.

Wylicza się go z użyciem następującego wzoru:

$$PR=((OR+OF)*OP)/(Z.TECH.+Z.ORG)$$

opis zastosowanych oznaczeń:

PR – poziom ryzyka

OR – wpływ na reputację

OF – oddziaływanie finansowe

OP – ocena prawdopodobieństwa wystąpienia zagrożenia (suma prawdopodobieństw)

Z.TECH. – poziom zabezpieczeń technicznych

Z.ORG. – poziom zabezpieczeń organizacyjnych

Próg akceptowalności ryzyka

Próg akceptowalności jest wyznaczany w oparciu o zasadę Pareto, zgodnie z którą 20% ryzyk o największej wartości punktowej jest przyczyną 80% pojawiających się zagrożeń i problemów w organizacji.

Matematyczny wzór do obliczenia wartości akceptowalności ryzyka to:

$$R.akceptowalne=(Rmax-Rmin)*0,8-Rmin$$

opis zastosowanych oznaczeń:

R.akcepotowalne – wartość progu akceptowalności ryzyka

Rmax – ryzyko o drugiej największej wartości (odrzucamy wartość skrajną)

Rmin – ryzyko o drugiej najmniejszej wartości (odrzucamy wartość skrajną)

WARIANT 2

Ocena poziomu ryzyka

Poziom ryzyka wyrażony jest w kategoriach kombinacji skutków oraz ich prawdopodobieństw. Wartość ryzyka jest wyliczana jako iloczyn średniej z prawdopodobieństw oraz sumy skutków:

$$PR=(OP/4)*(OF+OR)$$

opis zastosowanych oznaczeń:

PR – poziom ryzyka

OR – wpływ na reputację

OP – ocena prawdopodobieństwa wystąpienia zagrożenia

OF – oddziaływanie finansowe

		ODDZIAŁYWANIE NA FINANSE I NA REPUTACJĘ (**suma**)						
		2	3	4	5	6	7	8
PRAWDOPODOBIEŃSTWO (**średnia**)	1	2 (N)	3 (N)	4 (N)	5 (N)	6 (N)	7 (N)	8 (Ś)
	do 1,5	3 (N)	4,5	6 (N)	7,5 (Ś)	9 (Ś)	10,5 (Ś)	12 (Ś)
	do 2	4 (N)	6 (N)	8 (Ś)	10 (Ś)	12 (Ś)	14 (W)	16 (W)
	do 2,5	5 (N)	7,5 (Ś)	10 (Ś)	12,5 (W)	15 (W)	17,5 (W)	20 (W)
	do 3	6 (N)	9 (Ś)	12 (Ś)	15 (W)	18 (W)	21 (K)	24 (K)
	do 3,5	7 (N)	10,5 (Ś)	14 (W)	17,5 (W)	21 (K)	24,5 (K)	28 (K)
	do 4	8 (Ś)	12 (Ś)	16 (W)	20 (W)	24 (K)	28 (K)	32 (K)
	do 4,5	9 (Ś)	13,5 (W)	18 (W)	22,5 (K)	27 (K)	31,5 (K)	36 (K)
	do 5	10 (Ś)	15 (W)	20 (W)	25 (K)	30 (K)	35 (K)	40 (K)

Poziom ryzyka	Opis działania
Krytyczny (K) 21 - 40	Poziom ryzyka nietolerowany – wymaga natychmiastowego działania, zastosowania odpowiednich zabezpieczeń
Wysoki (W) 12,5 - 20	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga stałego monitorowania oraz zastosowania odpowiednich zabezpieczeń
Średni (Ś) 7,5 - 12	Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga monitorowania oraz zastosowania odpowiednich zabezpieczeń
Niski (N) do 7	Poziom ryzyka akceptowany – działania podejmowane w zależności od wymaganych nakładów

W przypadku poziomu ryzyka o wartości powyżej 7, musimy upewnić się, że stosujemy odpowiedni poziom zabezpieczeń. Do sprawdzenia, czy zastosowane zabezpieczenia są odpowiednie, musimy dokonać obliczenia:

Zabezpieczenia=Z.TECH*Z.ORG.

opis zastosowanych oznaczeń:

Zabezpieczenia – wartość zastosowanych zabezpieczeń

Z.TECH. – poziom zabezpieczeń technicznych

Z.ORG. – poziom zabezpieczeń organizacyjnych

		ZABEZPIECZENIA ORGANIZACYJNE			
		1,5	3	4,5	6
ZABEZPIECZENIA TECHNICZNE	1,5	2,25 (N)	4,5 (N)	6,75 (N)	9 (Ś)
	3	4,5 (N)	9 (Ś)	13,5 (W)	18 (W)
	4,5	6,75 (N)	13,5 (W)	20,25 (K)	27 (K)
	6	9 (Ś)	18 (W)	27 (K)	36 (K)

Poziom zastosowanych zabezpieczeń powinien plasować się na tym samym poziomie, lub wyższym, co poziom ryzyka. To oznacza, że np. dla wysokiego poziomu ryzyka, o wartościach między 12,5-20, poziom naszych zabezpieczeń również powinien plasować się w tych wartościach.

PRZYKŁADOWA KARTA ANALIZY RYZYKA – WARIANT I

NAZWA GRUPY AKTYWÓW (ZASOBÓW)	
NAZWA AKTYWA (ZASOBU)	
WŁAŚCICIEL AKTYWA (ZASOBU)	

PODATNOŚĆ AKTYWA (ZASOBU)	

PRZETWARZANIE DANYCH WRAŻLIWYCH (ART.9 UST. 1 RODO)	

OCENA PRAWDOPODOBIEŃSTWA WYSTĄPIENIA ZAGROŻENIA (OP)		
1	Zniszczenia fizyczne i naturalne (Z.1)	
2	Utrata podstawowych usług i awarie techniczne (Z.2)	
3	Naruszenia bezpieczeństwa informacji (Z.3)	
4	Nieautoryzowane działania i naruszenia bezpieczeństwa funkcji, w tym zagrożenia osobowe zewnętrzne (Z.4)	
	SUMA (1-4)	
ZASTOSOWANE ZABEZPIECZENIA		
1	Zabezpieczenia techniczne (Z.TECH.)	
2	Zabezpieczenia organizacyjne (Z.ORG.)	
	SUMA (1-2)	
	ODDZIAŁYWANIE NA FINASNE SZKOŁY (OF)	
	ODDZIAŁYWANIE NA REPUTACJĘ SZKOŁY (OR)	
	POZIOM RYZYKA DLA ZASOBU	
	AKCEPTOWALNY POZIOM RYZYKA DLA ZASOBU	

PRZYKŁADOWA KARTA ANALIZY RYZYKA – WARIANT II

NAZWA GRYPY AKTYWÓW (ZASOBÓW)	
NAZWA AKTYWA (ZASOBU)	
WŁAŚCICIEL AKTYWA (ZASOBU)	

PODATNOŚĆ AKTYWA (ZASOBU)	

OCENA PRAWDOPODOBIEŃSTWA WYSTĄPIENIA ZAGROŻENIA (OP)		
1	Zniszczenia fizyczne i naturalne (Z.1)	
2	Utrata podstawowych usług i awarie techniczne (Z.2)	
3	Naruszenia bezpieczeństwa informacji (Z.3)	
4	Nieautoryzowane działania i naruszenia bezpieczeństwa funkcji, w tym zagrożenia osobowe zewnętrzne (Z.4)	
	ŚREDNIA (1-4)	
1	**ODDZIAŁYWANIE NA FINASNE SZKOŁY (OF)**	
2	**ODDZIAŁYWANIE NA REPUTACJĘ SZKOŁY (OR)**	
	SUMA (1-2)	
ZASTOSOWANE ZABEZPIECZENIA		
1	**Zabezpieczenia techniczne (Z.TECH.)**	
2	**Zabezpieczenia organizacyjne (Z.ORG.)**	
	ILOCZYN (1-2)	
	POZIOM RYZYKA DLA AKTYWA (ZASOBU)	
	POZIOM STOSOWANYCH ZABEZPIECZEŃ	

III.POSTĘPOWANIE Z RYZYKIEM

Kolejną czynnością, jaką należy wykonać po oszacowaniu ryzyka dla poszczególnych operacji przetwarzania, jest podjęcie decyzji dotyczącej poszczególnych ryzyk.

Przykładowo w normie ISO/IEC 27005 wyróżnia się 4 możliwe rodzaje postępowań. Są to:

1) **modyfikowanie (redukcja) ryzyka** – polega na obniżeniu poziomu ryzyka (np. poprzez zmianę prawdopodobieństwa wystąpienia określonego zdarzenia lub zmniejszenie skutków jego wystąpienia). Na przykład zmniejszenie prawdopodobieństwa wystąpienia zdarzenia spowodowanego przerwą w dostawie energii można osiągnąć, włączając w układ zasilania odpowiednią automatykę i niezależne źródła energii (UPS-y, generatory). Zaś zmniejszenie związanych z tym zdarzeniem skutków utraty danych można osiągnąć, modyfikując system wykonywania kopii z wersji, w której kopia wykonywana jest jeden raz na dobę, do postaci, w której kopia jest wykonywana co 15 minut lub w sposób ciągły (na bieżąco) poprzez zastosowanie dodatkowych zabezpieczeń lub modyfikację procedur w sposób pozwalający na zaakceptowanie ryzyka szczątkowego;

2) **zachowanie (akceptacja) ryzyka** – to świadoma i obiektywna decyzja o niewprowadzaniu żadnych zmian w działaniu organizacji (zabezpieczeń), jeżeli poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka;

3) **unikanie ryzyka** – polega na unikaniu przez organizację działań, które powodują powstanie określonych typów ryzyka, np. w przypadku, gdy zidentyfikowane ryzyka są zbyt wysokie lub koszt wdrożenia zabezpieczeń nie jest adekwatny do zysków;

4) **dzielenie (przeniesienie) ryzyka** – polega na wykupieniu ubezpieczenia od jakiegoś zdarzenia lub scedowaniu skutków ryzyka na kontrahenta (np. podwykonawcę); należy pamiętać, że przeniesienie ryzyka nie eliminuje go. Trzeba zaznaczyć, że zgodnie z przepisami ogólnego rozporządzenia o ochronie danych wykupienie ubezpieczenia nie wyeliminuje ryzyka niezastosowania się przez dany podmiot do przepisów RODO. Ponadto administrator w sytuacji, kiedy zleca innym podmiotom przetwarzanie danych, to jako podmiot decydujący o zakresie i celach tego przetwarzania, ponosi pełną odpowiedzialność za zgodne z prawem przetwarzanie wskazanych danych.

Należy mieć na uwadze, że szczególnym przypadkiem jest sytuacja, gdy organizacja nie jest świadoma ryzyka i wobec tego nieświadomie wystawia się na nie w pełnym zakresie.

IV. Kategorie zabezpieczeń (ISO 27001 i ISO 27002)

LP.	KATEGORIA ZABEZPIECZEŃ	ZALECENIA
1	Polityka bezpieczeństwa informacji	Zaleca się, aby zbiór polityk bezpieczeństwa został określony, zatwierdzony przez dyrektora, zakomunikowany pracownikom i właściwym stronom zewnętrznym
2	Organizacja bezpieczeństwa informacji	Zaleca się, aby odpowiedzialność za bezpieczeństwo informacji była określona i przypisana
3	Bezpieczeństwo zasobów ludzkich	Zaleca się zweryfikowanie historii wszystkich kandydatów do pracy, zgodnie z odpowiednimi przepisami, regulacjami i zasadami etycznymi oraz proporcjonalnie do wymagań szkoły, klasyfikacji informacji do których będzie potrzebny dostęp oraz dostrzeżenie ryzyk
4	Zgodność	Dla każdego systemu informatycznego oraz całej szkoły zaleca się zidentyfikowanie, udokumentowanie i aktualizowanie wszystkich istotnych wymagań prawnych, regulacyjnych, umownych oraz podejścia szkoły do ich przestrzegania
5	Kontrola dostępu	Zaleca się ustanowienie, udokumentowanie i poddawanie okresowym przeglądom praw dostępu użytkowników do zasobów
6	Szyfrowanie danych	Zaleca się opracowanie i wdrożenie polityki stosowania zabezpieczeń kryptograficznych do ochrony informacji
7	Bezpieczeństwo fizyczne i środowiskowe	Zaleca się określenie granic bezpieczeństwa i wykorzystania ich w celu zabezpieczenia obszarów zawierających wrażliwe lub krytyczne informacje
8	Bezpieczna eksploatacja	Zaleca się, aby procedury eksploatacyjne były udokumentowane i udostępnione wszystkim potrzebującym ich użytkownikom
9	Zarządzanie aktywami	Zaleca się zidentyfikowanie aktywów, związanych z informacjami i środkami przetwarzania informacji oraz sporządzenie i utrzymanie ewidencji tych aktywów
10	Bezpieczna komunikacja	Zaleca się, aby sieci były zarządzane i nadzorowane w celach ochrony informacji w systemach informatycznych
11	Relacje z dostawcami	Zaleca się uzgodnienie z dostawcą i udokumentowanie wymagań bezpieczeństwa informacji celem zmniejszenia ryzyka związanego z dostępem dostawcy do aktywów szkoły
12	Zarządzanie incydentami	Zaleca się ustanowienie i odpowiedzialność kierownictwa oraz procedur zapewniających szybką, skuteczną i zorganizowaną reakcję na incydenty związane z bezpieczeństwem informacji
13	Ciągłość działania	Zaleca się, określenie przez szkołę wymagań dotyczących bezpieczeństwa informacji i ciągłości zarządzania

		bezpieczeństwem informacji w niekorzystnych sytuacjach np. w czasie kryzysu, braku energii elektrycznej

ZASADY PRZETWARZANIA DANYCH W IMIENIU ADMINISTRATORA

Przepisy RODO określają szczególne wymagania w zakresie przetwarzania dokonywanego przez podmioty przetwarzające w imieniu administratora danych. Niniejszy dokument określa zasady stosowane w jednostce w przypadku zlecania przetwarzania danych podmiotowi trzeciemu.

Powierzenie przetwarzania danych podmiotom trzecim, które będą przetwarzać je w imieniu administratora jest możliwe wyłącznie po przeprowadzeniu stosownych analiz, w tym oceny podmiotu, w sytuacji, kiedy Dyrekcja ma przekonanie, że podmiot ten zapewnia wystarczające gwarancje wdrożenia i stosowania odpowiednich i skutecznych środków bezpieczeństwa.

Analiza wstępna

Każdorazowo przeprowadza się analizę wstępną, obejmującą procesy przetwarzania danych, w ramach których rozważane jest skorzystanie z usług podmiotu trzeciego. Analiza ta dokonywana jest z uwzględnieniem:

- powodów, dla których rozważa się powierzenie przetwarzania danych,
- korzyści uzyskiwane w przypadku powierzenia przetwarzania danych,
- ryzyka związane z powierzeniem przetwarzania danych w tym konkretnym przypadku,
- możliwe alternatywy.

Efektem przeprowadzonej analizy wstępnej powinna być decyzja dotycząca powierzenia przetwarzania danych w ramach określonych procesów lub odstąpienie od takiego powierzenia.

Analiza podmiotu

Na etapie wyboru podmiotu, który będzie przetwarzał dane w imieniu administratora dokonuje się oceny podmiotu.

Oceny podmiotu dokonuje się z wykorzystaniem Karty oceny podmiotu, stanowiącej załącznik do niniejszych Zasad.

Umowa

Przetwarzanie danych w imieniu administratora ma miejsce wyłącznie na podstawie zawartej umowy.

Umowę zawiera się w formie pisemnej. W szczególnych przypadkach – po zasięgnięciu dodatkowej opinii prawnej – dopuszcza się zawarcie umowy w formie innej niż pisemna (np. elektronicznej), co jest jednak rozwiązaniem nierekomendowanym.

Zawierana umowa musi spełniać wymogi przepisów RODO, w szczególności art. 28.

Standard zapisów umownych, który powinien być stosowany stanowi załącznik do niniejszych Zasad.

KARTA OCENY PODMIOTU

POD KĄTEM ZLECENIA MU PRZETWARZANIA DANYCH OSOBOWYCH NA GRUNCIE ART. 28 RODO

DANE ADMINISTRATORA DANYCH	
Nazwa	
Adres	
Imię i nazwisko Inspektora Ochrony Danych	
CEL I CHARAKTER ZLECENIA PRZETWARZANIA DANYCH	
Jakie dane będą podlegały przetwarzaniu przez podmiot trzeci?	
W jakim celu będą one przetwarzane przez ten podmiot?	
Jaki jest spodziewany okres przetwarzania danych przez ten podmiot?	
DANE IDENTYFIKACYJNE OCENIANEGO PODMIOTU	
Nazwa	
Adres	
Nr NIP lub REGON	
CECHY I SYTUACJA RYNKOWA PODMIOTU	
Forma prawna podmiotu	
Czy przetwarzanie danych jest związane z działalnością zarobkową podmiotu	
Od kiedy podmiot działa?	
Orientacyjna liczba aktualnych Klientów	
Jaka jest wielkość podmiotu? (np. wielkość rocznego przychodu, liczba pracowników)	
Jaka jest pozycja firmy na rynku, w tym rynku lokalnym/regionalnym?	
Czy podmiot figuruje w rejestrze dłużników?	
Czy w podmiocie wyznaczono Inspektora Ochrony Danych?	

DOŚWIADCZENIA I OPINIE	
Czy współpracowaliśmy już z tym podmiotem? Jeśli tak, to jakie mamy doświadczenia?	
Czy znamy inną jednostkę podobną do nas, która współpracowała z tym podmiotem? Jeśli tak, to jakie są jej doświadczenia?	
Jakie są opinie o tym podmiocie osób bezpośrednio nam znanych?	
Jakie są opinie o tym podmiocie pochodzące z niezidentyfikowanych źródeł (tzw. obiegowe opinie)	
UMOWA I SPOSÓB REALIZACJI	
Czy umowa z podmiotem, która ma być zawarta gwarantuje: 1. Możliwość kontrolowania przez nas procesu przetwarzania danych po stronie podmiotu, w szczególności niezwłoczne udzielanie wszelkich informacji? 2. Odpowiednio szybkie przekazywanie informacji o naruszeniach? (rekomendowane 24 godziny, maksymalnie 48 godzin) 3. Otwartość oraz zobowiązanie się do współpracy? 4. Zobowiązanie do wsparcia przy realizacji żądań kierowanych do administratora na podst. art. 32-36 RODO? 5. Zobowiązanie do stosowania przepisów RODO przez ten podmiot? 6. W przypadku korzystania z podwykonawców wzięcie pełnej odpowiedzialności przez podmiot za działania swoich podwykonawców oraz zapewnienie gwarancji, że spełniają oni wymogi RODO?	
Czy podmiot zapewnia wsparcie w zakresie obowiązków administratora, w szczególności możliwości wykazania spełniania wymogów RODO, dotyczących przedmiotu współpracy?	
Z jakiego rodzaju podwykonawców podmiot korzysta? (jakie czynności wykonuje osobiście, a jakie zleca podwykonawcom) Jaka jest ich liczba? Czy ci podwykonawcy zapewniają należyty poziom bezpieczeństwa i spełniają wymogi RODO?	
Czy podmiot będzie przetwarzał dane na terenie państw trzecich? (w szczególności poza Europejskim Obszarem Gospodarczym)	
INNE INFORMACJE	

DODATKOWE UWAGI DO OCENY

Na podstawie przeprowadzonej analizy, uznaje się, że wskazany na wstępie podmiot

zapewnia wystarczające gwarancje / nie zapewnia wystarczających gwarancji*

wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

…….. ……

data

……..

podpis osoby przeprowadzającej analizę

* - niepotrzebne skreślić.

UMOWA

PRZETWARZANIA DANYCH OSOBOWYCH

(DAWNIEJ POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH)

W dniu …….. umowę zawierają:

……. z siedzibą ……., zwana/y dalej *Administratorem danych*. *Administratora danych* reprezentuje:

…….. – dyrektor

oraz

……, z siedzibą …….., zwana dalej *Przetwarzającym*. *Przetwarzającego* reprezentuje:

…….. – ……..

§1
KONTEKST ZAWARCIA UMOWY

1. Niniejsza umowa jest zawierana w związku z następującą umową lub umowami:
   a. …
   b. …
   zwanymi łącznie *Umową odrębną*.
2. Celem zawarcia niniejszej umowy jest uregulowanie wzajemnych zobowiązań stron w związku z przetwarzaniem danych osobowych w ramach realizacji Umowy odrębnej oraz zadośćuczynienie wymogom prawnym, w szczególności 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) (Dz. Urz. UE, L 119 z 4.05.2016), zwanego dalej *RODO*.

§2
DANE, KTÓRYCH DOTYCZY UMOWA

Umowa objęte są dane osobowe przetwarzane w ……..

<w tym miejscu należy określić, jakie dane są przedmiotem umowy, czyli np. dane przetwarzane w systemie X>

§3
CHARAKTER DOSTARCZANYCH PRODUKTÓW I ŚWIADCZONYCH USŁUG

<w tym miejscu powinien zostać określony ewentualny szczególny charakter produktów lub usług dostarczanych przez dostawcę przetwarzającego dane, mogący mieć wpływ na przetwarzanie danych lub sposób realizacji uprawnień administratora danych. W szczególności w tym miejscu należy określić, czy przedmiotem umowy odrębnej jest produkt lub usługa oferowane masowo, czy świadczenia indywidualne, dedykowane wyłącznie administratorowi danych>

§4
PRZEDMIOT I CZAS TRWANIA PRZETWARZANIA

1. Przedmiotem przetwarzania danych osobowych w ramach niniejszej umowy jest realizacja *Umowy odrębnej*, w szczególności ….. *<warto w tym miejscu wskazać kluczowy przedmiot umowy odrębnej>*.
2. Czas przetwarzania danych jest ograniczony do okresu obowiązywania niniejszej umowy, z zastrzeżeniem mechanizmów związanych z usuwaniem danych, w tym usuwaniem kopii zapasowych, które określono w §14.

3. ….*<inne uregulowania dotyczące czasu obowiązywania umowy, na przykład zasady jego przedłużenia w przypadku zawarcia kolejnej, analogicznej umowy odrębnej>*… .

§5
CHARAKTER I CEL PRZETWARZANIA

1. Przetwarzanie danych w ramach realizacji niniejszej umowy ma charakter ciągły, jest wykonywane w formie elektronicznej z wykorzystaniem narzędzi informatycznych, w tym w szczególności systemów, o których mowa w §2 i jest związane z realizacją przez *Przetwarzającego Umowy odrębnej*.
2. Przetwarzanie o charakterze opisanym w ust. 1 obejmuje wykonywanie na danych takich czynności jak odczytywanie, zapisywanie, przechowywanie, przesyłanie, sporządzanie kopii zapasowych lub serwisowych.
3. Ponadto w celu rozwoju oraz optymalizacji wydajności dostarczanych rozwiązań, a także w celu wykrycia potencjalnych zagrożeń, w szczególności prób włamania lub innej nielegalnej działalności *Przetwarzający* może prowadzić analizy aktywności użytkowników i sposobu posługiwania się przez nich systemem. Prowadzone analizy mają charakter statystyczny i nie powodują utrwalenia po stronie *Przetwarzającego* danych umożliwiających identyfikację użytkowników, z wyjątkiem sytuacji podejrzenia wystąpienia incydentu bezpieczeństwa bądź podejrzenia prowadzenia działań nielegalnych.

   <Powyżej zaprezentowano przykład dla umowy obejmującej przetwarzanie danych w systemach informatycznych, co jest najczęstszym przypadkiem. W sytuacji, gdy umowa dotyczy innego rodzaju przetwarzania, powyższe zapisy należy dostosować odpowiednio do sytuacji, wskazując charakter przetwarzania oraz podstawowe czynności wykonywane w ramach przetwarzania.>

4. Celem przetwarzania danych przez *Przetwarzającego* w ramach niniejszej umowy jest realizacja *Umowy odrębnej*.

   <w tym miejscu umowa może zostać uzupełniona o ewentualne dodatkowe ustalenia dotyczące charakteru lub celów przetwarzania, np. zasady wykorzystania dostarczanych rozwiązań>

§6
RODZAJ DANYCH OSOBOWYCH

W ramach niniejszej umowy będą przetwarzane rodzaje danych opisane w Załączniku nr 1 do niniejszej umowy.

§7
KATEGORIE OSÓB, KTÓRYCH DANE DOTYCZĄ

W ramach niniejszej umowy będą przetwarzane dane dotyczące kategorii osób wymienionych w Załączniku nr 1 do niniejszej umowy.

§8
MIEJSCE PRZETWARZANIA DANYCH

Przetwarzający oświadcza, iż w ramach realizacji niniejszej umowy dane osobowe będą przetwarzane wyłącznie na terytorium Rzeczpospolitej Polskiej/Europejskiego Obszaru Gospodarczego.

§9
PODMIOTY, Z USŁUG KTÓRYCH KORZYSTA PRZETWARZAJĄCY

1. *Administrator danych* wyraża zgodę na korzystanie przez *Przetwarzającego* z usług firm ...*<w tym miejscu wskazanie firm, z usług których chce korzystać Przetwarzający>*… w zakresie …*<w tym miejscu określenie zakresu, w jakim Przetwarzający zamierza przy realizacji umowy korzystać z tych podwykonawców>*….
2. W przypadku, gdy *Przetwarzający* uzna, że w celu prawidłowej realizacji niniejszej umowy potrzebuje korzystać zakresie wskazanym w ust. 1 z usług innego podmiotu niż te wymienione w ust. 1, wówczas informuje *Administratora danych* o nazwie i adresie nowego podmiotu.
3. Strony ustalają, że jeżeli *Administrator danych* w ciągu 14 (czternastu) dni od otrzymania informacji, o której mowa w ust. 2 nie zgłosi pisemnego sprzeciwu oznacza to zgodę *Administratora danych* na korzystanie przez *Przetwarzającego* przy realizacji niniejszej umowy z usług tego podmiotu.

4. *Przetwarzający* gwarantuje, że podmioty wskazane w ust. 1 zapewniają poziom bezpieczeństwa danych, w tym spełniają wymogi prawne, odpowiadające wszystkim postanowieniom niniejszej umowy. Ponadto *Przetwarzający* oświadcza, że w przypadku zmian, realizowanych w trybie ust. 2 i 3 również będzie korzystał z usług wyłącznie takich podmiotów.
5. Korzystanie przez *Przetwarzającego* przy realizacji niniejszej umowy z usług innych podmiotów jest możliwe wyłącznie po uprzednim uzyskaniu zgody *Administratora danych*, zgodnie z art. 28 ust. 2 *RODO*.
6. Za wszystkie działania lub zaniechania podmiotów, z których usług przy realizacji niniejszej umowy korzysta *Przetwarzający* ponosi on odpowiedzialność wobec *Administratora danych* jak za własne działania lub zaniechania.

§10
INCYDENTY

1. *Przetwarzający* w przypadku stwierdzenia naruszenia ochrony danych osobowych przetwarzanych w ramach realizacji niniejszej umowy bez zbędnej zwłoki zgłasza ten fakt *Administratorowi danych*.
2. Przetwarzający przekazuje zgłoszenie, o którym mowa w ust. 1 nie później niż 36 (trzydzieści sześć) godzin od momentu stwierdzenia naruszenia. Zgłoszenie, o którym mowa jest przekazywane za pośrednictwem poczty elektronicznej na adres kontaktowy *Administratora danych*, wskazany w §17 ust. 1 lit. a oraz za pomocą wiadomości SMS, jeżeli wśród danych *Administratora danych* został podany numer telefonu komórkowego.

   <powyższe należy traktować jako propozycję sposobu informowania. Strony powinny ustalić, w jaki sposób administrator danych będzie informowany w przypadku wystąpienia naruszenia>

3. Dodatkowo poza przekazaniem informacji o fakcie stwierdzenia naruszenia ochrony danych osobowych, w przekazanej za pośrednictwem poczty elektronicznej wiadomości, o której mowa w ust. 2 *Przetwarzający* przekazuje informacje dotyczące stwierdzonego naruszenia, obejmujące:
   a. charakter naruszenia, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   b. wskazanie możliwych konsekwencji naruszenia;
   c. opis zastosowanych środków, jakie *Przetwarzający* zastosował w celu zaradzenia naruszeniu bądź zminimalizowania jego ewentualnych negatywnych skutków oraz ewentualne sugestie dla *Administratora danych* do zastosowania dalszych środków.
4. Jeżeli w momencie przekazywania informacji, o której mowa w ust. 3 *Przetwarzający* nie posiada wszystkich informacji, zobowiązuje się on uzupełniać je niezwłocznie po tym, jak będzie w stanie ich udzielić.
5. Uregulowania zawarte w niniejszym paragrafie stosuje się także do naruszeń stwierdzonych przez podmioty, z usług których korzysta *Przetwarzający* na mocy uregulowań §9. Odpowiedzialnym za przekazywanie informacji *Administratorowi danych* o naruszeniach stwierdzonych przez te podmioty jest *Przetwarzający*.
6. Naruszenia, o których mowa w niniejszym paragrafie rozumiane są zgodnie z definicją tego pojęcia zawartą w art. 4 pkt 12 RODO

§11
WSPÓŁPRACA ADMINISTRATORA DANYCH I PRZETWARZAJĄCEGO

1. *Administrator danych* i *Przetwarzający* zobowiązują się ściśle współpracować ze sobą w zakresie przetwarzania danych osobowych w ramach realizacji niniejszej umowy.
2. *Administrator danych* i *Przetwarzający* zobowiązują się niezwłocznie przekazywać sobie wzajemnie wszystkie informacje, które mogą mieć wpływ na bezpieczeństwo przetwarzania danych w ramach realizacji niniejszej umowy.

3. *Przetwarzający* jest zobowiązany do informowania *Administratora danych* o wszelkich czynnościach prowadzonych u niego w kontekście danych osobowych przetwarzanych w ramach realizacji niniejszej umowy przez uprawnione do tego organy państwa (Policję, prokuraturę, GIODO/PUODO itp.), w tym w szczególności o wnioskach dotyczących udostępnienia danych objętych niniejszą umową., chyba że przekazanie takiej informacji *Administratorowi danych* stanowiłoby naruszenie przepisów prawa powszechnie obowiązującego.

§12
OBOWIĄZKI PRZETWARZAJĄCEGO

1. *Przetwarzający* zobowiązuje się do zachowania tajemnicy treści danych osobowych przetwarzanych na podstawie niniejszej umowy, w tym w szczególności, że nie będzie on tych danych przekazywał ani ujawniał osobom nieuprawnionym oraz nie będzie wykorzystywał ich w celach innych niż wynikające z niniejszej umowy.
2. *Przetwarzający* zobowiązuje się do dopuszczenia do przetwarzania danych osobowych w ramach realizacji niniejszej umowy wyłącznie osoby, które zostały upoważnione do przetwarzania danych osobowych oraz zobowiązały się do zachowania tajemnicy.
3. *Przetwarzający* jest zobowiązany podjąć środki wymagane na mocy art. 32 *RODO*. Na żądanie *Administratora danych Przetwarzający* przedstawi, z zastrzeżeniem §13 informacje, dokumenty lub wyjaśnienia potwierdzające podjęcie środków, o których mowa w zdaniu pierwszym.
4. *Przetwarzający* – w zakresie, w jakim jest to związane z realizacją niniejszej umowy i w miarę posiadanych możliwości – zobowiązuje się pomagać *Administratorowi danych* w wywiązaniu się przez niego z realizacji obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania praw tej osoby określonych w rozdziale III *RODO*.
5. *Przetwarzający* – w zakresie, w jakim jest to związane z realizacją niniejszej umowy oraz w zakresie dostępnych mu informacji – zobowiązuje się pomagać *Administratorowi danych* w wywiązaniu się przez niego z obowiązków określonych w art. 32-36 *RODO*.
6. *Przetwarzający* zobowiązuje się przekazywać *Administratorowi danych* z własnej inicjatywy wszelkie informacje, które uzna za istotne z punktu widzenia przetwarzania danych w ramach realizacji niniejszej umowy lub ważne dla wypełniania przez *Administratora danych* jego obowiązków wynikających z przepisów prawa.
7. Przetwarzający zobowiązuje się przekazywać *Administratorowi danych* na jego żądanie wszelkie informacje, o które ten będzie wnioskował – o ile Przetwarzający będzie je posiadał – w zakresie przetwarzania danych osobowych w ramach realizacji niniejszej umowy, z zastrzeżeniem §13.

§13
TAJEMNICA PRZEDSIĘBIORSTWA

Przetwarzający zapewnia *Administratorowi danych* dostęp do wszystkich informacji dotyczących procesów przetwarzania danych osobowych, prowadzonych w ramach realizacji niniejszej umowy, po stronie *Przetwarzającego*. Jednakże w przypadku, gdy *Administrator danych* zwróci się o udzielenie informacji stanowiącej tajemnicę przedsiębiorstwa *Przetwarzającego* lub będącą informacją o szczególnym znaczeniu dla bezpieczeństwa przetwarzanych danych, której publiczne ujawnienie mogłoby spowodować zagrożenie dla bezpieczeństwa danych (np. szczegóły techniczne zastosowanej konfiguracji systemów lub zabezpieczeń), *Przetwarzający* udzieli żądanych informacji jedynie po uprzednim podpisaniu z *Administratorem danych* dodatkowej umowy o zachowaniu poufności oraz – jeżeli będzie to miało w danym przypadku zastosowanie – uzgodnieniu bezpiecznego kanału lub formy udostępnienia tej informacji.

<w tym miejscu może nastąpić ewentualne zastrzeżenie dostępu administratora danych do określonych informacji lub obwarowanie dostępu do nich dodatkowymi wymogami formalnymi. Należy zwrócić uwagę, by regulacja nie ograniczyła administratorowi danych dostępu do informacji związanych z bezpieczeństwem przetwarzania danych, a co za tym idzie uniemożliwiła nadzór nad prawidłową realizacją umowy.

Powyżej zaprezentowano przykład odnoszący się jedynie do obwarowania dostępu do informacji szczególnie chronionej z punktu widzenia dostawcy dodatkowymi wymogami formalnymi, natomiast nieograniczającymi możliwości zapoznania się administratora z tymi informacjami.>

§14
ZAKOŃCZENIE UMOWY, USUNIĘCIE (ZWROT) DANYCH

1. Niniejsza umowa zostaje zawarta na okres obowiązywania *Umowy odrębnej*.
2. W przypadku zakończenia trwania *Umowy odrębnej* lub niniejszej umowy z dowolnego powodu, *Powierzający* usunie dane przetwarzane na podstawie niniejszej umowy niezwłocznie, przy czym nie później niż w ciągu …*<określenie liczby dni>*… dni od daty zakończenia umowy.
3. *Powierzający* usunie także wszystkie posiadane kopie zapasowe danych. Usunięcie wszystkich kopii zapasowych nastąpi najpóźniej …*<określenie liczby dni>*… dni od daty zakończenia umowy, na co *Administrator danych* wyraża zgodę.

<w tym miejscu mogą pojawić się dodatkowe uregulowania dotyczące sytuacji, trybu lub warunków zakończenia niniejszej umowy>

§15
KONTROLA

1. *Administrator danych* jest uprawniony do kontrolowania procesu przetwarzania danych objętych niniejszą umową przez *Przetwarzającego* przez cały okres obowiązywania niniejszej umowy i na zasadach w niej określonych.

<W tym miejscu należy określić zasady, na jakich administrator danych może prowadzić kontrolę procesu przetwarzania. Należy pamiętać, że można stosować różne formy kontroli – od uzyskiwania wyjaśnień i odpowiedzi na zadane pytania, po kontrole bezpośrednio u wykonawcy. Zasady, na jakich kontrola może być prowadzona powinny zostać opisane w tej części umowy>

§16
WYŁĄCZENIA ODPOWIEDZIALNOŚCI

1. *Przetwarzający* nie ponosi odpowiedzialności za skutki niepodjęcia działań przez *Administratora danych* lub podjęcia przez niego działań niewłaściwych w zakresie obowiązków i odpowiedzialności *Administratora danych*. W szczególności *Przetwarzający* nie ponosi odpowiedzialności za stosowane po stronie *Administratora danych* środki bezpieczeństwa oraz sposoby ich doboru, jak i prowadzoną dokumentację.

<W tym miejscu powinny zostać określone ewentualne inne wyłączenia odpowiedzialności przetwarzającego – np. skutki posługiwania się oprogramowaniem niezgodnie z jego przeznaczeniem, niestosowanie się do zasad lub zaleceń dotyczących bezpieczeństwa itp.>

§17
KONTAKTY

1. W celu umożliwienia lub ułatwienia realizacji niniejszej umowy strony wskazują następujące dane kontaktowe:
   a. *Administrator danych* (dyrektor) – imię i nazwisko: ….., numer telefonu: ….., numer telefonu komórkowego: ….., adres e-mail: ….., adres do korespondencji tradycyjnej: ……
   b. Inspektor ochrony danych u *Administratora danych* – imię i nazwisko: …., numer telefonu: …., numer telefonu komórkowego: ….., adres e-mail: ……
   c. *Przetwarzający*: numer telefonu – ……., adres e-mail: ……, adres do korespondencji tradycyjnej: ……..
   d. Inspektor ochrony danych u *Przetwarzającego* – imię i nazwisko……., numer telefonu: ……, adres e-mail: ……..
2. W przypadku zmiany danych kontaktowych wskazanych w niniejszym paragrafie, strony zobowiązują się niezwłocznie poinformować drugą stronę o zmianie, wskazując aktualne dane kontaktowe.

§18
INNE POSTANOWIENIA

1. W przypadku naruszenia przez *Przetwarzającego* przepisów prawa powszechnie obowiązującego w związku z realizacją niniejszej umowy, w wyniku czego *Administrator danych* zostanie obciążony karą pieniężną nałożoną przez organ nadzorczy lub prawomocnie zobowiązany do wypłaty odszkodowania, w zakresie jakim będą one wynikały z winy *Przetwarzającego*, *Przetwarzający* zobowiązuje się pokryć poniesione przez *Administratora danych* z tego tytułu straty. Warunkiem poniesienia odpowiedzialności, o której mowa w zdaniu poprzednim, jest poinformowanie *Przetwarzającego* o wszczęciu postępowania i w przypadku wyrażenia takiej woli przez *Przetwarzającego* umożliwienie mu udziału w postępowaniu, o ile będzie to zgodne z przepisami prawa.
2. Niniejsza umowa stanowi udokumentowanie polecenie administratora do przetwarzania danych, o którym mowa w art. 28 ust. 3 lit. a *RODO*.
3. Umowa podlega prawu polskiemu. W sprawach nieuregulowanych umową mają zastosowanie przepisy prawa powszechnie obowiązującego w Polsce.
4. Wszelkie zmiany lub uzupełnienia umowy wymagają formy pisemnej pod rygorem nieważności.
5. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.
6. Umowa obowiązuje od dnia zawarcia.

Podpisując niniejszy egzemplarz umowy potwierdzam, że nie zawiera on żadnych skreśleń ani ręcznych poprawek w treści umowy.

……
……..
Administrator danych

Podpisując niniejszy egzemplarz umowy potwierdzam, że nie zawiera on żadnych skreśleń ani ręcznych poprawek w treści umowy.

……
……..
Przetwarzający

Załączniki:

1. Rodzaj danych oraz kategorie osób, których dane są przetwarzane w ramach umowy.