FORMIKA
FLEXO PRINTING

POLITYKA BEZPIECZEŃSTWA INFORMACJI

E S G

...ponieważ to nasza odpowiedzialność wobec planety

FORMIKA
FLEXO PRINTING

POLITYKA BEZPIECZEŃSTWA INFORMACJI

METRYKA DOKUMENTU:

TYTUŁ	**POLITYKA BEZPIECZEŃSTWA INFORMACJI W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH**
AUTORZY	Gabriela Cieplicka, Kancelaria Ochman i Partnerzy
WERSJA DOKUMENTU	1.0
DATA ZATWIERDZENIA	16.09.2024
ZATWIERDZIŁ	Paweł Gurgul
DATA OSTATNIEGO PRZEGLĄDU	----------
CZASOOKRES PRZEGLĄDU	Nie rzadziej niż co 24 miesiące lub w przypadku istotnych zmian w przepisach, standardach branżowych oraz strukturze organizacyjnej.
STATUS	Obowiązujący
SPOSÓB UPUBLICZNENIA	Publikacja na stronie www.formika.com.pl, ujawnienia w raporcie Zrównoważonego Rozwoju zgodnego z Rozporządzeniem ESRS, materiały informacyjne dla pracowników.
ABSTRAKT	Polityka Bezpieczeństwa Informacji określa standardy i zasady postępowania, które mają na celu ochronę praw osób fizycznych i prawnych przed nieuprawnionym przetwarzaniem danych oraz zapewnienie, że dane te będą przetwarzane zgodnie z poszanowaniem przepisów prawnych. Polityka określa także zaangażowane środki techniczne i organizacyjne, które minimalizują ryzyko wycieku, nieuprawnionego dostępu lub innych incydentów związanych z bezpieczeństwem danych. Polityka określa cele jakościowe i ilościowe zmierzające do osiągnięcia ogólnych założeń polityki oraz alokacje środków przeznaczonych na ich realizację.
ODPOWIEDZIALNY ZA WDROŻENIE	Prezes Zarządu

POLITYKA BEZPIECZEŃSTWA INFORMACJI

SPIS TREŚCI:

POLITYKA BEZPIECZEŃSTWA INFORMACJI

1. Postanowienia ogólne

§ 1. Cel Polityki

Celem Polityki Bezpieczeństwa danych osobowych, zwanej dalej PolitykąBezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, 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 (zwane dalej „RODO") w zakresie ochrony danych osobowych, sposobu przetwarzania informacji zawierających dane osobowe w Formika Sp. z o.o.

§ 2. Określenia użyte w Polityce Bezpieczeństwa oznaczają:

1. Jednostka – Formika Sp. z o.o. z siedzibą w Brwinowie (zwana dalej również jako „Spółka Formika");
2. Dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane olokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
3. Przetwarzanie danych osobowych- oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
4. Użytkownik – osoba upoważniona do przetwarzania danych osobowych;

POLITYKA BEZPIECZEŃSTWA INFORMACJI

5. Administrator systemu – osoba upoważniona do zarządzania systemem informacyjnym;
6. System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
7. Zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą.

2. Definicja Bezpieczeństwa Informacji

§ 3.

1. Utrzymanie bezpieczeństwa przetwarzanych przez Jednostkę informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z zasobem stanowiącym przedmiot niniejszej Polityki.
2.Poniżej opisane jest rozumienie wyżej wymienionych pojęć w odniesieniu do informacji i aplikacji:
1) Poufność informacji – rozumiana jako zapewnienie, że tylko uprawnieni pracownicy mają dostęp do informacji,
2) Integralność informacji – rozumiana jako zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania,
3) Dostępność informacji – rozumiane jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne,
4) Zarządzanie ryzykiem– rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych.
3.Dodatkowo zarządzanie bezpieczeństwem informacji wiąże się z zapewnieniem:
1) Niezaprzeczalności odbioru – rozumianej jako zdolność systemu do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie,
2) Niezaprzeczalności nadania – rozumianej jako zdolność systemu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie,
3) Rozliczalności działań – rozumianej, jako zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie i możliwym jest zidentyfikowanie użytkownika, który działania dokonał.

.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

3. Zakres

§ 4.

1. W systemie informacyjnym Jednostki przetwarzane są informacje służące do wykonywania zadań niezbędnych dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisów prawa.
2. Informacje te są przetwarzane i składowane zarówno w postaci manualnej jak i elektronicznej.

§ 5.

Politykę Bezpieczeństwa stosuje się do:
1.Danych osobowych przetwarzanych w systemie informatycznym,
2. Wszystkich informacji dotyczących danych pracowników i współpracowników Jednostki, w tym danych osobowych personelu i treści zawieranych umów o pracę,
3. Wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji,
4. Danych członków rodzin pracowników i współpracowników oraz osób trzecich,
5. Wszystkich danych kontrahentów i klientów przed oraz po zawarciu umowy o współpracy,
6. Informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
7. Rejestru osób dopuszczonych do przetwarzania danych osobowych,
8. Innych dokumentów zawierających dane osobowe.

§ 6.

1. Zakresy określone przez dokumenty Polityki Bezpieczeństwa Informacji mają zastosowanie do całego systemu informacyjnego Jednostki w szczególności do:
1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie,
2) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
3) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, współpracowników, stażystów i innych osób mających dostęp do informacji podlegających ochronie.
2. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, współpracownicy, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

§ 7.

Informacje niejawne nie są objęte zakresem niniejszej Polityki.

4. Struktura dokumentów Polityki Bezpieczeństwa Informacji

§ 8.

1. Polityka Bezpieczeństwa Informacji ustanawia metody zarządzania oraz wymagania niezbędne do zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.
2. Zestaw dokumentów Polityki Bezpieczeństwa Informacji składa się z:
1) Niniejszego dokumentu Polityki Bezpieczeństwa Informacji,
2) Instrukcji zarządzania systemem informatycznym w zakresie wymogów bezpieczeństwa przetwarzania danych osobowych, opisującej sposób zarządzania systemami przetwarzania danych osobowych w Jednostce,
3) Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych, opisującej tryb postępowania w sytuacjach naruszenia zabezpieczenia zasobów danych osobowych, zaobserwowanych prób naruszenia tego zabezpieczenia, a także uzasadnionego podejrzenia o przygotowywanej próbie naruszenia.

5. Dostęp do informacji

§ 9.

1. Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, podlegają przeszkoleniu w zakresie obowiązujących przepisów prawa dotyczących ochrony danych osobowych oraz obowiązujących w Jednostce zasad ochrony danych osobowych.

§ 10.

Zakres czynności dla osoby dopuszczonej do przetwarzania danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę danych osobowych w stopniu odpowiednim do zadań tej osoby realizowanych przy przetwarzaniu tych danych.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

§ 11.

Udostępnianie danych osobowych podmiotom uprawnionym do ich otrzymania na podstawie przepisów prawa jest możliwe, jeżeli podmioty te wiarygodnie uzasadnią potrzebę posiadania tych danych, a ich przekazanie nie naruszy praw i wolności osób, których dane dotyczą.

§ 12.

Pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.

§ 13.

Dane osobowe udostępnia się na pisemny, umotywowany wniosek, który powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać zakres i przeznaczenie.

6. Zarządzanie danymi osobowymi

§ 14.

Administratorem danych osobowych jest Formika Spółka z o.o. z siedzibą w Brwinowie.

§ 15.

Administrator danych osobowych dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest zobowiązany zapewnić, aby dane osobowe były:

1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;

§ 15.

5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy RODO w celu ochrony praw i wolności osób, których dane dotyczą;
6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Administrator jest odpowiedzialny za przestrzeganie zasad wskazanych powyżej i jest w stanie wykazać ich przestrzeganie.

7. Zakresy odpowiedzialności

§ 16.

Za bezpieczeństwo informacji oraz ochronę zasobów danych osobowych Jednostki jako całości przed ich nieuprawnionym użyciem lub zniszczeniem odpowiedzialny jest każdy pracownik Jednostki.

§ 17.

Administrator w Jednostce:
1. odpowiada za realizację ustawy o ochronie danych osobowych,
2. sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których dane są przetwarzane oraz kontrolą przebywających w nich osób,
3. określa strategię zabezpieczania systemów informatycznych Jednostki,
4. sprawuje nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
5. sprawuje nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych na których zapisane są dane osobowe,

POLITYKA BEZPIECZEŃSTWA INFORMACJI

§ 17.

6. identyfikuje i analizuje zagrożenia oraz ryzyko, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych Jednostki,
7. określa potrzeby w zakresie zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe,
8. sprawuje nadzór nad bezpieczeństwem danych zawartych w komputerach przenośnych, dyskach wymiennych, w których przetwarzane są dane osobowe,
9. sprawuje nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe,
10. monitoruje działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych,
11. sprawuje nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych,
12. zatwierdza wnioski o przyznaniu danemu użytkownikowi identyfikatora oraz praw dostępu do informacji chronionych w danym systemie przetwarzania,
13. powiadamia o konieczności utworzenia identyfikatora użytkownika w systemie oraz zmianie/nadaniu uprawnień dostępu użytkownika do systemu,
14. prowadzi ewidencję baz danych w systemach informatycznych, w których przetwarzane są dane osobowe,
15. prowadzi ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych,
16. prowadzi ewidencję miejsc przetwarzania danych osobowych w systemach informatycznych,
17. prowadzi rejestr zbiorów danych osobowych Jednostki (przetwarzanych metodą tradycyjną lub w systemach informatycznych).

POLITYKA BEZPIECZEŃSTWA INFORMACJI

§ 18.

Administrator danych osobowych zobowiązany jest do przestrzegania wszystkich przepisów prawa, w szczególności poprzez:
1. określanie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z ustawy o ochronie danych osobowych i RODO,
2. określenie budynków, pomieszczeń lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego,
3. zapoznawanie osób zatrudnionych przy przetwarzaniu danych osobowych z przepisami obowiązującymi w tym zakresie,
4. wdrażanie i nadzorowanie przestrzegania Polityki bezpieczeństwa informacji,
5. wdrażanie i nadzorowanie przestrzegania instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
6. działanie zgodnie z instrukcją postępowania w sytuacji naruszenia ochrony danych osobowych,
7. stwarzanie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z obowiązywania ustawy o ochronie danych osobowych,
8. odpowiedzialność za poprawność merytoryczną danych gromadzonych w systemach informacyjnych,
9. określanie, które osoby i na jakich prawach mają dostęp do danych informacji.

§ 19.

Administrator w zakresie funkcjonowania Systemu Informatycznego odpowiedzialny jest za:
1. bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
2. optymalizację wydajności systemu informatycznego, baz danych,
3. instalacje i konfiguracje sprzętu sieciowego i serwerowego,
4. instalacje i konfiguracje oprogramowania systemowego i sieciowego,
5. konfigurację i administracje oprogramowaniem systemowym i sieciowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,
6. współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
7. zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego,
8. zarządzanie kopiami awaryjnymi danych w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
9. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
10. przyznawanie ściśle określonych praw dostępu do informacji w danym systemie,
11. zarządzanie licencjami, procedurami ich dotyczącymi,
12. prowadzenie profilaktyki antywirusowej.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

8. Przetwarzanie danych osobowych

§ 20.

1. Administrator może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych oraz przetwarzać dane na zlecenie innego podmiotu.
2. Powierzenie przetwarzania danych przez Administratora następuje w szczególności w przypadkach umów outsourcingowych, których wykonanie wymaga przetwarzania danych osobowych w imieniu i na rzecz Administratora, a także w przypadkach udostępniania przez Administratora danych osobowych osób zatrudnionych podmiotom trzecim, takim jak centra medyczne świadczące usługi zdrowotne na rzecz pracowników i firmy oferujące pozapłacowe świadczenia pracownicze.
3. Administrator powierzając przetwarzanie danych osobowych korzysta z usług takich dostawców, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dotyczą. Administrator wybierając podmiot przetwarzający dane, zwraca uwagę na standardy bezpieczeństwa przez niego stosowane lub też wyznacza wymagany przez siebie standard (np. za pomocą audytów czy innych form sprawdzenia).
4. Powierzenie przetwarzania odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii Europejskiej lub prawu państwa członkowskiego, a zasady, na których podstawie następuje powierzenie wyczerpują wymagania zawarte w art. 28 RODO.
5. Osoby zatrudnione przez podmiot wykonujący umowę na rzecz Administratora i osoby, za których pośrednictwem podmiot ten wykonuje czynności w ramach tej umowy, mogą zostać zobowiązane przez Administratora, do złożenia oświadczenia o zachowaniu poufności.

§ 21.

Administrator dopuszcza przetwarzanie danych osobowych, gdy został spełniony co najmniej jeden z poniższych warunków:
1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych przez Administratora w jednym lub większej liczbie określonych celów (np. marketingu produktów i usług);
2) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze (np. przepisów związanych z zatrudnieniem i ubezpieczeniami społecznymi);
4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

POLITYKA BEZPIECZEŃSTWA INFORMACJI

§ 21.

5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym;
6) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem (np. marketingu własnych produktów i usług wobec jego klientów czy oceny rocznej pracowników).

§ 22.

1. Zgoda, o której jest mowa w §21 pkt 1 może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania.

2. Za prawnie uzasadniony interes, o którym mowa w ust §21 pkt 6, uważa się w szczególności:
1) marketing bezpośredni własnych produktów lub usług.
2) dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

3. Zgody klienta wymaga marketing po wygaśnięciu umowy Klienta z Administratorem (np. w przypadku prób nakłonienia byłego klienta do ponownego zawarcia umowy), a także gdy klient wystąpił o zawarcie umowy lecz nie została ona zawarta;

4. Przez zgodę osoby, której dane dotyczą, należy rozumieć dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych. Do wyraźnych działań wskazujących na wyrażenie zgody np. przez klienta zaliczyć można w szczególności wybór przez klienta ustawień technicznych systemu informatycznego, przekazanie przez klienta ustnie, pisemnie lub za pomocą elektronicznych środków komunikacji stosowanych przez Administratora swoich danych osobowych.

5. Za wyrażenie zgody nie uznaje się m.in. milczenia osoby, braku sprzeciwu, niepodjęcia przez nią działań oraz zaznaczenia domyślnie okienek wyboru w systemie informatycznym.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

§ 22.

6. Zgody nie uważa się za wyrażoną świadomie lub dobrowolnie, m.in. jeśli:
1) od wyrażenia przez osobę zgody uzależnione jest wykonanie umowy, w tym świadczenie usług, a do wykonania tej umowy zgoda nie jest niezbędna;
2) osoba nie ma możliwości udzielenia osobnej zgody na różne cele przetwarzania danych w przypadkach, kiedy jest to stosowne, np. osobna zgoda na przetwarzanie danych w celach marketingowych,
3) zapytanie o zgodę nie zostało przedstawione w sposób pozwalający wyraźnie odróżnić go od pozostałych kwestii, w przypadku gdy treść zgody na przetwarzanie danych zawarta jest w pisemnym oświadczeniu, które zawiera również inne treści, np. klauzula zgody na przetwarzanie danych osobowych zawarta w treści umowy pomiędzy Administratorem a klientem.
7. Jeśli zgoda osoby ma stanowić wyłączną podstawę prawną przetwarzania danych w określonym celu lub celach, wyrażenie zgody przez osobę powinno nastąpić przed faktycznym rozpoczęciem przetwarzania.
8. Udzielone przez klienta zgody dotyczące przetwarzania danych mogą zostać przez niego w każdym czasie odwołane ze skutkiem natychmiastowym. Odwołanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.
9. Administrator zbierając zgodę od osoby lub oświadczenie o wycofaniu zgody, powinien upewnić się, że osoba wyrażająca/wycofująca zgodę jest w rzeczywistości osobą, której dane dotyczą.

9. Obowiązek informacyjny z art. 13 i art. 14 RODO

§ 23.

Jednym z podstawowych obowiązków towarzyszących zbieraniu danych osobowych jest obowiązek informacyjny, wynikający z art. 13 RODO (zbieranie danych bezpośrednio od osoby, której dane dotyczą) oraz art. 14 RODO (zbieranie danych nie bezpośrednio od osoby, której one dotyczą).

POLITYKA BEZPIECZEŃSTWA INFORMACJI

§ 24.

1.Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, Administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:
1)swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
2) dane kontaktowe inspektora ochrony danych;
3) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
4) jeżeli przetwarzanie odbywa się na podstawie prawnie uzasadnionego interesu Administratora lub strony trzeciej – prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią;
5) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
6) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych;
7) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
8) informacje o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
9) jeżeli przetwarzanie odbywa się na podstawie zgody podmiotu danych(art. 6 ust. 1 lit. a)lub art. 9 ust. 2 lit. a) RODO) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
10) informacje o prawie wniesienia skargi do organu nadzorczego;
11) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
12) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

§ 24.

2. Jeżeli Administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji.
3. W przypadku zbierania danych osobowych bezpośrednio od osoby, której dane dotyczą, Administrator przekazuje informacje podczas pozyskiwania danych.

§ 25.

1.Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, Administrator podaje osobie, której dane dotyczą, następujące informacje:
1) swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
2) dane kontaktowe inspektora ochrony danych;
3) cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania;
4) kategorie odnośnych danych osobowych;
5) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
6) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych;
7) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
8) jeżeli przetwarzanie odbywa się na podstawie prawnie uzasadnionego interesu Administratora lub strony trzeciej – prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią;
9) informacje o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

POLITYKA BEZPIECZEŃSTWA INFORMACJI

§ 25.

10) jeżeli przetwarzanie odbywa się na podstawie zgody podmiotu danych(art. 6 ust. 1 lit. a)lub art. 9 ust. 2 lit. a) RODO) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
11) informacje o prawie wniesienia skargi do organu nadzorczego;
12) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;
13) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
2. Informacje, o których mowa w ust.1, Administrator podaje:
1) w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca –mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
2) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą –najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
3) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.
3. Jeżeli Administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji.
4. Informacje mogą być przekazywane m.in. jako klauzule informacyjne zawarte w dokumentach przeznaczonych dla osoby, której dane dotyczą, klauzule informacyjne w systemie informatycznym, ustna informacja przekazana przez konsultanta, po potwierdzeniu tożsamości osoby, której dane dotyczą, czy też informacja przekazana drogą elektroniczną z zastosowaniem zasad bezpieczeństwa. Informacje mogą być opatrzone standardowymi znakami graficznymi.
5. Odstępstwa od wypełnienia obowiązku informacyjnego w stosunku do osoby, której dane dotyczą, są możliwe, jeśli m.in.:
1) podmiot danych posiada stosowne informacje;
2) udzielenie informacji osobie, której dane zostały zebrane nie bezpośrednio od niej, jest niemożliwe lub wymagałoby niewspółmiernego dużego wysiłku albo wymagałoby pozyskiwania informacji dodatkowych z innych źródeł zewnętrznych. W sytuacji nie udzielenia osobie informacji ze względu na powyższe.
3) pozyskanie lub ujawnienie danych osoby, której dane są zebrane nie bezpośrednio od niej, uregulowane jest w przepisach prawa przewidujących ochronę prawnie uzasadnionych interesów osoby, której dane dotyczą;
4) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnic ustawowo chronionych.

§ 25.

4) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnic ustawowo chronionych.
6. Administrator zapewnia rozliczalność w zakresie realizacji lub braku realizacji obowiązków informacyjnych w szczególności poprzez zbieranie dokumentów przekazywanych osobom zawierające klauzule informacyjne, rejestrację rozmów telefonicznych, backup'y/zrzuty z ekranu systemu informatycznego, kopie listów lub wiadomości wysyłanych drogą elektroniczną do podmiotu danych zawierających klauzule informacyjne, analizy oraz procedury wewnętrzne, skrypty rozmów z klientami.

10. Prawa osoby fizycznej (klienta, pracownika, etc.) w zakresie ochrony danych osobowych

§ 26.

1. Każda osoba, której dane przetwarza Administrator, w ramach przysługującego jej praw wskazanych w rozdzialeIII RODO, jest uprawniona do skorzystania z praw wskazanych w rozdziale III RODO i opisanych poniżej.
2. Podmiot danych jest uprawniony do zgłoszenia żądania, o którym mowa w punktach poniżej w formie pisemnej lub elektronicznej. Nie wyłącza to uprawnienia Klienta do złożenia żądania w innej akceptowalnej i możliwej do udokumentowania.
3. W każdym przypadku żądanie podmiotu danych powinno wskazywać, jakich danych osobowych i czynności dotyczy. W przypadku, gdy żądanie jest nieprecyzyjne, w tym nie zawiera wskazania zakresu danych osobowych i czynności, jaka objęta jest wnioskiem, Administrator zwraca się do Klienta o przekazanie takich informacji.
4. W przypadku braku sprecyzowania przez podmiot danych jakich danych i jakich czynności żądanie dotyczy, Administrator jest uprawniony do wstrzymania realizacji żądania do momentu uzyskania wystarczających informacji od Klienta. Administrator realizuje żądanie podmiotu danych zgodnie ze swoimi wewnętrznymi procedurami. Odpowiednie procedury postępowania w przypadku skorzystania przez podmiot danych z przysługujących mu praw zostały wskazane w następnych punktach.
5. Realizacja praw osoby, której dane dotyczą, przez Administratora następuje w rozsądnym terminie uwzględniającym koszty, stopień trudności realizacji żądania oraz w oparciu o wewnętrzne procesy funkcjonujące u Administratora.
6. Administrator poinformuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania każdego odbiorcę, któremu ujawnił dane osobowe osoby, której dane dotyczą.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

§ 27. Prawo dostępu do jej danych osobowych

1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji w zakresie:
1) celów przetwarzania;
2) kategorii danych osobowych;
3) informacji o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
4) w miarę możliwości, informacji o planowanym okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteriów ustalania tego okresu;
5) informacji o prawie do żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
6) informacji o prawie wniesienia skargi do organu nadzorczego;
7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkich dostępnych informacji o ich źródle;
8) informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem.
3. Administrator dostarczy osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, Administrator pobiera opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych.
4. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, Administrator udziela informacji drogą elektroniczną.
5. Prawo do uzyskania kopii nie może niekorzystnie wpływać na prawa i wolności innych.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

§ 28. Prawo do sprostowania danych

1. Osoba, której dane dotyczą, ma prawo żądania od Administrator sprostowania dotyczących go danych osobowych, które są nieprawidłowe.
2. Osoba, której dane dotyczą ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

§ 29. Prawa do usunięciadanych („prawo do bycia zapomnianym")

1. Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a Administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
2) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO i nie ma innej podstawy prawnej przetwarzania;
3) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO (marketing bezpośredni) wobec przetwarzania;
4) dane osobowe były przetwarzane niezgodnie z prawem;
5) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Polskim lub UE;
6) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 RODO.
2. Jeżeli Administrator upublicznił dane osobowe, a ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.
3. Prawo do bycia zapomnianym nie ma zastosowania, w zakresie w jakim przetwarzanie jest niezbędne m.in.:
1) do korzystania z prawa do wolności wypowiedzi i informacji;
2) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Polskiego lub Unii Europejskiej lub do wykonania zadania realizowanego w interesie publicznym;
3) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, o ile prawdopodobne jest, że prawo do bycia zapomnianym uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
4) do ustalenia, dochodzenia lub obrony roszczeń.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

§ 30. Prawa do ograniczenia przetwarzania danych

1. Osoba, której dane dotyczą, ma prawo żądania od Administratora ograniczenia przetwarzania w następujących przypadkach:
1) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;
2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
3) Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
4) osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.
2. Jeżeli przetwarzanie danych zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy Polskiego lub unijnego interesu publicznego.
3. Przed uchyleniem ograniczenia przetwarzania Administrator informuje o tym osobę, której dane dotyczą.

§ 31. Prawo do przenoszenia danych

1. Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła Administratorowi oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony Administratora, któremu dostarczono te dane osobowe, jeżeli:
1) przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) RODO lub art. 9 ust. 2 lit. a) RODO lub na podstawie umowy w myśl art. 6 ust. 1 lit. b) RODO; oraz
2) przetwarzanie odbywa się w sposób zautomatyzowany.
2. Wykonując prawo do przenoszenia danych , osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez Administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.
3. Wykonanie prawa do przenoszenia danych pozostaje bez uszczerbku dla prawa do usunięcia danych.

§ 32. Prawo do sprzeciwu

1. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na uzasadnionym interesie prawnym administratora danych lub gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
2. Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.
3. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych Administratorowi nie wolno już przetwarzać danych do takich celów.
4. Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie do sprzeciwu oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.

11. Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności przetwarzania danych

§ 33.

W Jednostce rozróżnia się następujące kategorie środków zabezpieczeń danych osobowych:
1. Zabezpieczenia fizyczne:
1) pomieszczenia zamykane na klucz,
2) szafy z zamkami,
2. Zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:
1) przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach,
2) przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby.
3. Zabezpieczenia organizacyjne:
1) osobą odpowiedzialną za bezpieczeństwo danych jest Administrator
2) Administrator na bieżąco kontroluje pracę systemu informatycznego z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i z obowiązującymi procedurami,
4. Organizacja pracy przy przetwarzaniu danych osobowych i zasady przetwarzania:
1) wykaz pracowników Jednostki uprawnionych do przetwarzania danych osobowych, znajduje się u Administratora,

POLITYKA BEZPIECZEŃSTWA INFORMACJI

12. Okres retencji danych osobowych przetwarzanych przez administratora

§ 34.

1. Administrator działając zgodnie z art. 5 ust. 1 pkt. e RODO przechowuje dane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.
2. Dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO.
3. Po osiągnięciu zamierzonych (pierwotnych) celów przetwarzania, dane osobowe osób, których dane dotyczą, powinny zostać usunięte, chyba, że ich dalsze przechowywanie znajduje podstawę prawną (np. w ustawie z dnia 29 września 1994 r. o rachunkowości, ustawie z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa)
4. Usunięcie danych osobowych osób, których dane dotyczą następuje poprzez ich zniszczenie.

13. Zarządzanie dokumentacją

§ 35.

1. Zasady składowania: wszystkie dokumenty materialne będą przechowywane w dedykowanych, zabezpieczonych miejscach z ograniczonym dostępem. Lokacje będą wyposażone w systemy monitoringu oraz zabezpieczenia przeciwpożarowe. Dokumenty będą przechowywane zgodnie z wewnętrznymi przepisami dotyczącymi okresów przechowywanie oraz obowiązującymi regulacjami prawnymi.
2. Dostęp do dokumentów bieżących będzie kontrolowany poprzez system uprawnień, który pozwoli na wgląd do dokumentacji jedynie uprawnionym pracownikom. Każdy dostęp do dokumentów będzie rejestrowany, a ewidencja będzie przechowywana w sposób umożliwiający późniejsze audyty.
3. Dostęp do archiwów: Dokumenty nieaktualne lub o mniejszym znaczeniu operacyjnym będą przenoszone do archiwów zgodnie z procedurami archiwizacji. Archiwa będą objęte dodatkowymi zabezpieczeniami fizycznymi i elektronicznymi, takimi jak systemy alarmowe, kontrola dostępu oraz regularne przeglądy.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

§ 35.

4. Zarządzanie korespondencją mailową i dokumentacją elektroniczną:
–Serwery i infrastruktura IT:
Opis serwerów;
Zabezpieczenia elektroniczne i fizyczne: zabezpieczenie fizycznego dostępu do sieci komputerowej oraz zabezpieczenie ruchu w sieci komputerowej:

- Zarządzanie dostępem urządzeń do sieci LAN/WIFI (802.1x).
- Filtrowanie ruchu przychodzącego/wychodzącego na urządzeniach sieciowych brzegowych – BIAŁE/CZARNE listy.
- IDS/IPS.
- Segmentacja sieci.
- Monitoring urządzeń oraz reakcja na zdarzenia.

- Zasady zarządzania korespondencją mailową:
Filtrowanie i ochrona: wszelka korespondencja mailowa będzie poddawana filtrowaniu antywirusowemu oraz antyspamowemu, wiadomości mailowe będą zabezpieczone za pomocą szyfrowania.
- Polityka retencji danych:
E-maile zawierające poufne informacje będą przechowywane zgodnie z polityką retencji danych, a po upływie ustalonego czasu usuwane albo archiwizowane.

– Zarządzanie dokumentacją w formie elektronicznej:
a) Przechowywanie dokumentów:
wszystkie dokumenty elektroniczne będą przechowywane na serwerach Spółki Formika, które są odpowiednio zabezpieczone.
b) Kopie zapasowe: Regularnie będą tworzone kopie zapasowe dokumentów, które zostaną przechowywane w bezpiecznych lokalizacjach zgodnie z procedurami Spółki Formika.
c) Dostęp do dokumentacji: dostęp do elektronicznej dokumentacji będzie kontrolowany przez systemy autoryzacji i uwierzytelniania, aby zapewnić, że tylko uprawnieni pracownicy mogą uzyskać dostęp do poufnych informacji.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

14. Pozostałe postanowienia

§ 36.

Spółka Formika zobowiązuje się do zapewnienia bezpiecznego zbierania, przetwarzania i przechowywania informacji osób trzecich na potrzeby biznesowe. Rozumiejąc wagę ochrony poufnych informacji, implementujemy najwyższe standardy bezpieczeństwa, aby chronić dane przed nieautoryzowanym dostępem, ujawnieniem, zmianą czy zniszczeniem. Niniejsza polityka stanowi integralną część Polityki Etyki Biznesowej, Code of Conduct, Podręcznika Pracownika, a także jest uwzględniona w Raportach Rocznych oraz Raportach dotyczących Zrównoważonego Rozwoju.

1. Cele i założenia Polityki:

Założeniem Polityki jest zapewnienie bezpieczeństwa informacji, co ma bezpośredni wpływ na cele jakościowe i ilościowe. Przeprowadzenie oceny ryzyka IT na 100% wszystkich obiektów do roku 2030 zwiększy zdolności do zarządzania ryzykiem i ochroną poufnych danych.
Cele zostały ustalone na podstawie analizy ryzyka przeprowadzonej we współpracy z zewnętrznymi audytorami oraz wewnętrznymi ekspertami ds. bezpieczeństwa IT. Wykorzystano dane dotyczące incydentów bezpieczeństwa oraz analizy scenariuszy z raportów IPCC.

Cele jakościowe:

- Pełne zobowiązanie do odpowiedzialnego i zgodnego z najlepszymi praktykami zarządzania poufnymi informacjami,
- Zwiększenie świadomości w zakresie bezpieczeństwa informacji – regularne szkolenia dla wszystkich pracowników Spółki Formika w zakresie aktualnych zagrożeń związanych z bezpieczeństwem informacji oraz najlepszych praktyk w zakresie ochrony danych,
- Zobowiązanie do przestrzegania wszystkich obowiązujących przepisów prawa dotyczących ochrony danych oraz bezpieczeństwa informacji.

Cele ilościowe:

- Przeprowadzenie kompleksowej oceny ryzyka bezpieczeństwa IT we wszystkich obiektach i systemach, którą są częścią infrastruktur IT do roku 2030,
- Dla monitorowania realizacji powyższych celów Formika ustanowiła następujące kluczowe wskaźniki (KPI):
- Liczba zgłoszonych przypadków incydentów związanych z naruszeniem bezpieczeństwa informacji, liczba bazowa dla roku 2022 wynosi 0 przypadków;
- Celem jest utrzymanie tego wskaźnika na poziomie 0,
- Wskaźnik przeszkolenia (liczba osób przeszkolonych do całkowitej ilości pracowników)
- Rokiem bazowym jest rok 2022.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

2. Wykluczenia: Polityka nie obejmuje przetwarzania danych niepoufnych (np. ogólnych informacji marketingowych), informacji przed podmioty zewnętrzne, które nie podlegają bezpośredniej kontroli spółki Formika sp. z o. o.
3. Osobą odpowiedzialną za wdrożenie i nadzór nad realizacją polityki jest Prezes Zarządu spółki Formika sp. z o. o.
4. Polityka odnosi się do następujących standardów i przepisów:

- ISO/IEC 27001:2013
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

5. Interesariuszami zaangażowanymi w tworzenie i wdrożenie Polityki są: pracownicy, klienci, dostawy usług IT, audytorzy zewnętrzni. Przeprowadzone zostały konsultacje zgodnie ze standardem AA1000 SES, które wykazały, że kluczowymi kwestiami dla interesariuszy są:

- ochrona danych osobowych,
- zapewnienie ciągłości działania systemów informatycznych,
- przejrzystość w zakresie procedur bezpieczeństwa.

6. Polityka jest udostępniona na stronie internetowej spółki Formika sp. z o. o.
7. Metody ustalania celów:
8. Wsparcie dla osób poszkodowanych: w przypadku incydentów naruszenia danych, firma zapewnia wsparcie poszkodowanym, w tym bezpłatną pomoc prawną oraz pomoc techniczną w zabezpieczeniu ich danych osobowych.

Prezes Zarządu deklaruje przeznaczanie niezbędnych środków inwestycyjnych (CAPEX) oraz operacyjnych (OPEX) na działania niezbędne do realizacji niniejszej polityki.
O postępie w realizacji celów informowany jest Zarząd na cyklicznych spotkaniach.
Za wdrożenie założeń polityki na poziomie operacyjnym odpowiedzialni są szefowie poszczególnych pionów operacyjnych.