Polityka bezpieczeństwa przetwarzania danych osobowych

DTI Polska

Dat/ Podpis zatwierdzającego	*Obowiązuje od:* **06.11.2023**

Rozdział 1

Postanowienia ogólne

§ 1. Niniejszy dokument (zwany w dalszej części: Polityka Bezpieczeństwa) opisuje reguły dotyczące bezpieczeństwa procesu przetwarzania danych osobowych w **DTI Polska M.Rogala sp.k., z siedzibą w Krakowie przy ul. Sobieskiego 1 m2.**

§ 2. Administratorem danych, w rozumieniu 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 (tzw. RODO) oraz USTAWY z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z dnia 2018-05-24 poz. 1000) jest **DTI Polska M.Rogala sp.k., z siedzibą w Krakowie przy ul. Sobieskiego 1 m2.**

§ 3. Realizacja postanowień Polityki Bezpieczeństwa ma zapewnić ochronę danych osobowych, właściwą ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa procesów przetwarzania danych osobowych oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w organizacji.

§ 4. Administrator jest odpowiedzialny za przeszkolenie każdego pracownika, który ma zostać upoważniony do przetwarzania danych osobowych, z zakresu ochrony danych osobowych oraz za zapoznanie go z Polityką Bezpieczeństwa i innymi wewnętrznymi regulacjami dotyczącymi ochrony danych osobowych.

Rozdział 2.

Definicje wybranych sformułowań dotyczących RODO

1) „**administrator**" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
2) „**dane osobowe**" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
3) „**przetwarzanie**" 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) „**profilowanie**" oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
5) „**pseudonimizacja**" oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
6) „**zbiór danych osobowych**" oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
7) **„Inspektor ochrony Danych(lub „IOD")** – podmiot (osoba fizyczna lub prawna) wspierający Administratora w realizacji obowiązków dotyczących ochrony danych osobowych.;
8) **„podmiot przetwarzający"** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
9) „**odbiorca**" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe;
10) „**strona trzecia**" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
11) „**zgoda**" osoby, której dane dotyczą oznacza 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;
12) „**naruszenie ochrony danych osobowych**" oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

13) „**dane biometryczne**" oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
14) „**dane dotyczące zdrowia**" oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
15) **„organ nadzorczy"** - Urząd Ochrony Danych Osobowych
16) „**transgraniczne przetwarzanie**" oznacza: a) przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności jednostek organizacyjnych w więcej, niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim; albo b)przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim;
17) **„Administratorze systemów informatycznych (lub „ASI")"** – rozumie się przez to osobę fizyczną wyznaczoną przez Administratora, która odpowiada za zapewnienie sprawności, należytej konserwacji i wdrażania technicznych zabezpieczeń systemów informatycznych oraz odpowiada za to, aby systemy informatyczne, w których przetwarzane są dane osobowe spełniały wymagania przewidziane ustawą i rozporządzeniem. W przypadku niewyznaczenia ASI, jego obowiązki wykonuje osobiście Administrator lub za pośrednictwem pracowników lub współpracowników wewnętrznej służby informatycznej lub podmiotu zewnętrznego, działającego na zlecenie Administratora.
18) **„upoważnieniu do przetwarzania danych osobowych"** – rozumie się przez to oświadczenie nadawane przez Administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu;
19) **„osoba upoważniona do przetwarzania danych osobowych"** – osobę, która otrzymała od Administratora upoważnienie do przetwarzania danych osobowych;
20) **„identyfikatorze (loginie) użytkownika"** — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
21) **„użytkownik systemu"** – rozumie się przez to osobę upoważnioną, która otrzymała dostęp do sieci LAN umożliwiający korzystanie z sieci Internet oraz login i hasło do systemu;

Rozdział 3.
Przetwarzanie danych

§ 5. O celach przetwarzania danych osobowych decyduje Administrator.

§ 6. Przetwarzanie danych jest dopuszczalne gdy:
   a) osoba, której dane dotyczą wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych;
   b) jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;
   c) jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;
   d) jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;
   e) jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez Administratora albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą;

§ 7. Zgoda na przetwarzanie danych osobowych:
   a) nie może być domniemana lub dorozumiana;
   b) nie może wynikać z oświadczenia woli o innej treści;
   c) może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania;
   d) może zostać odwołana w każdym czasie. W przypadku odwołania zgody na przetwarzanie danych osobowych Administrator obowiązany jest usunąć wszystkie dane osobowe osoby, która zgodę cofnęła, chyba że istnieje inna podstawa prawna upoważniająca Administratora do dalszego przetwarzania tych danych dla innych celów niż wskazany w cofniętej zgodzie;

§ 8. Zaleca się odbieranie zgody w postaci możliwej do późniejszego udowodnienia (np. pisemnie). W ramach systemu informatycznego po zastosowaniu metody dwustopniowego uwiarygodniania, jako nagranie przeprowadzonej rozmowy telefonicznej - po poinformowaniu rozmówcy o prowadzonej rejestracji).

§ 9. W przypadku powzięcia jakichkolwiek wątpliwości co do ewentualnej zgodności z prawem planowanych działań w zakresie przetwarzania danych, należy zwrócić się do administratora z wnioskiem o rozstrzygnięcie wątpliwości. Przed udzieleniem przez Administratora odpowiedzi w przedmiocie istniejących wątpliwości niedozwolone jest zbieranie danych osobowych i ich utrwalanie, a w przypadku

posiadania już danych osobowych których wątpliwość dotycz należy, do czasu rozstrzygnięcia wątpliwości, wstrzymać wszystkie działania na danych osobowych, co do których istnieją wątpliwości czy są prawnie uzasadnione.

Rozdział 4.

Zabezpieczenie przetwarzania danych osobowych

§ 10. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, Administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania –wdraża odpowiednie środki techniczne i organizacyjne, których zakres powinien wynikać z przeprowadzonej analizy ryzyka.

§ 11. Dopuszczane do przetwarzania danych osobowych są jedynie osoby, które uzyskały indywidualne upoważnienia do przetwarzania danych osobowych.

§ 12. Obszary, na którym dochodzi do przetwarzania danych osobowych, określono w **załączniku do niniejszego dokumentu**. Sposób zabezpieczenia obszarów wynika z analizy ryzyka.

§ 13. Z podmiotami, którym Administrator powierzył przetwarzanie danych osobowych, podpisywane są umowy na piśmie o powierzeniu przetwarzania danych osobowych. W zakresie pozostałych umów stosuję się klauzule o zachowaniu poufności.

§ 14. Podstawowe zasady zabezpieczenia danych osobowych:

a) wszelkie dokumenty zwierające dane osobowe przechowywane są w szafach lub pomieszczeniach zamykanych na klucz;
b) osoba będąca dysponentem kluczy nie może przekazywać kluczy do budynków i pomieszczeń, w których przetwarzane są dane osobom nieuprawnionym, a ponadto obowiązana jest przedsięwziąć działania celem wykluczenia ryzyka ich utraty;
c) osoba która utraciła posiadane klucze do pomieszczeń Administratora, w których przetwarzane są dane, niezwłocznie zgłasza tą okoliczność przełożonemu, który ma obowiązek podjąć wszelkie niezbędne środki techniczne i organizacyjne w celu zabezpieczenia pomieszczenia, do którego klucze utracono oraz powiadomić Administratora;
d) osoba przetwarzająca dane po zakończeniu pracy porządkuje swoje stanowisko, zabezpieczając dokumenty i nośniki elektroniczne z danymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach;
e) niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki gwarantującej odpowiedni stopień rozdrobnienia;
f) każdy dokument nieużyteczny zawierający dane należy zniszczyć niezwłocznie.
g) podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu (dotyczy to również dokumentów powstałych na skutek kopiowania bądź skanowania).
h) przebywanie osób trzecich w obszarze, w którym przetwarzane są dane jest dopuszczalne za zgodą Administratora lub w obecności osoby upoważnionej.

§ 15. Sposób zabezpieczenia danych osobowych przetwarzanych w systemach informatycznych został opisany w „Instrukcji zarządzania systemem informatycznym”.

Rozdział 5.

Opis zdarzeń naruszających bezpieczeństwo przetwarzania danych osobowych

§ 16. Następujące kategorie zdarzeń stanowią zagrożenia, które mogą prowadzić do naruszenia bezpieczeństwa przetwarzania danych osobowych:

a) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) – ich występowanie może prowadzić do utraty, zniszczenia, uszkodzenia danych oraz infrastruktury technicznej służącej do ich przechowywania;
b) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki pracowników, awarie sprzętowe, błędy oprogramowania) – może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych;
c) zagrożenia zamierzone – świadome i celowe działania powodujące naruszenia poufności danych (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:
   - nieuprawniony dostęp do systemu z zewnątrz (włamanie);
   - nieuprawniony dostęp do systemu z jego wnętrza;
   - nieuprawnione przekazanie danych;
   - bezpośrednie zagrożenie materialnych składników systemu (np. kradzież sprzętu, dokumentów).

§ 17. Naruszenie lub podejrzenie naruszenia bezpieczeństwa przetwarzania danych osobowych następuje w szczególności w następujących sytuacjach:

a) losowe lub nieprzewidziane oddziaływania czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne itp.;
b) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;
c) awaria sprzętu lub oprogramowania, które wyraźnie wskazuje na umyślne działanie w kierunku naruszenia ochrony danych;
d) podejrzenie nieuprawnionej modyfikacji danych lub innego odstępstwa od stanu oczekiwanego;
e) naruszenie lub próby naruszenia zapisów, integralności systemu lub bazy danych w tym systemie;
f) ujawnienia nieautoryzowanych kont dostępu do systemu;
g) naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji.

§ 18. Za podejrzenie naruszenia ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia fizycznego miejsc przechowywania i przetwarzania danych osobowych, a w szczególności:

a) niezabezpieczone pomieszczenia;
b) nienadzorowane, otwarte szafy, biurka, regały;
c) niezabezpieczone urządzenia archiwizujące;
d) pozostawianie danych w nieodpowiednich miejscach – kosze, stoły itp.

Rozdział 6

Postępowanie przy naruszeniu danych osobowych

§ 19. Sposób postępowania w przypadku naruszenia danych osobowych został opisany w dokumencie „Procedura postępowania w sytuacji naruszenia ochrony danych osobowych.”

Rozdział 7.

Postanowienia końcowe

§ 20. Wobec pracowników, którzy uchybili obowiązkom wynikającym z Polityki Bezpieczeństwa, wszczyna się postępowanie z tytułu odpowiedzialności dyscyplinarnej pracowników. Poważne naruszenia obowiązków wynikających z Polityki Bezpieczeństwa mogą być uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych.

§ 21. Zastosowane kary dyscyplinarnej wobec pracownika, który uchybił obowiązkom wynikającym z Polityki Bezpieczeństwa, nie wyklucza odpowiedzialności karnej tej osoby.

Załącznik nr 1 do Polityki Bezpieczeństwa

Wykaz pomieszczeń w których są przetwarzane dane osobowe

Lp.	Adres budynku	Wykaz pomieszczeń
1	Kraków ul. Sobieskiego 1 m2	Pomieszczenie biurowe

Załącznik nr 2 do Polityki Bezpieczeństwa

Wzór upoważnienia do przetwarzania danych osobowych

UPOWAŻNIENIE nr …….

do przetwarzania danych osobowych

Z dniem …… upoważniam Panią/Pana ……..

numer PESEL: ……

zatrudnioną/-ego na stanowisku:……..

w DTI Polska M.Rogala sp.k., z siedzibą w Krakowie przy ul. Sobieskiego 1 m2, do przetwarzania danych osobowych w następujących zbiorach:

Zakres upoważnienia do przetwarzania danych osobowych (*)	1	2	3	4	5	6	7	8
	Zbiór danych kontaktowych	Zbiór dokumentów kadrowych i płacowych	Zbiór dokumentów księgowych	Zbiór umów z kontrahentami	Ewidencja osób upoważnionych do przetwarzania danych osobowych			

*zaznaczyć symbolem „X" zakres; pozostałe wykreślić znakiem „--"

Upoważnienie wydaje się na czas do jego odwołania, zmiany stanowiska albo rozwiązania lub wygaśnięcia umowy o pracę / współpracę.

Jednocześnie, wraz z nadanym upoważnieniem, zobowiązuję Panią/Pana do zachowania w tajemnicy danych osobowych, do których uzyska Pani/Pan dostęp podczas realizacji obowiązków służbowych lub zadań zleconych oraz sposobów ich zabezpieczenia. Dodatkowo, zobowiązuję Panią/Pana do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez Administratora procedur / instrukcji wewnętrznych.

Miejscowość/data — z up. Administratora

OŚWIADCZENIE

Oświadczam, iż zostałam/em zapoznana/y z przepisami dotyczącymi ochrony danych osobowych, w szczególności ROZPORZĄDZENIEM 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) oraz Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z dnia 2018-05-24 poz. 1000) oraz wdrożonymi do stosowania przez Administratora procedurami i instrukcjami dotyczącymi ochrony danych osobowych. Równocześnie, zobowiązuję się do zachowania w tajemnicy danych osobowych, do których uzyskam dostęp podczas realizacji obowiązków służbowych lub zadań zleconych oraz sposobów ich zabezpieczenia.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez Pracodawcę za ciężkie naruszenie obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1 Kodeksu Pracy lub za naruszenie przepisów karnych ww. ustawy o ochronie danych osobowych lub ciężkie naruszenie obowiązków umownych w przypadku umowy cywilnoprawnej.

Miejscowość/data — Podpis pracownika