Grudzień 2021

POLITYKA BEZPIECZEŃSTWA INFORMACJI

MIASTOPROJEKT WROCŁAW SP. Z O.O.

Miastoprojekt Wrocław Sp. z o.o. ul. Snopkowa 2b, 52 – 225 Wrocław
tel. +48 71 342 92 93, e-mail: biuro@miastoprojektwroclaw.pl

WSTĘP

ROLA INFORMACJI W DZIAŁALNOŚCI GOSPODARCZEJ

Współczesne prowadzenie działalności gospodarczej opiera się na pozyskiwaniu, przetwarzaniu i wymianie informacji dotyczących kontrahentów, szczegółów handlowych, danych osobowych, tajemnicy przedsiębiorstwa oraz innych informacji, które posiadają wartość gospodarczą dla nas lub naszych kontrahentów. Szczególną wagę przywiązujemy do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa, głównie RODO. Takie informacje stanowią informacje niejawne, a ich ujawnienie może się odbywać wyłącznie przy wcześniejszym określeniu celu, zasadności ich przekazania oraz na warunkach określonych w umowie, a także przy zastosowaniu zasad ochrony przetwarzania takich informacji.

BEZPIECZEŃSTWO PRZETWARZANYCH INFORMACJI

Rola przetwarzanych informacji staje się coraz większa, przez co naszym zadaniem jest zapewnienie bezpieczeństwa tych informacji przed nieuprawnionym dostępem oraz utratą ich poufności lub integralności. Te 3 cechy (dostępność, poufność i integralność) stanowią fundament bezpieczeństwa informacji, który jest priorytetem w działalności Miastoprojekt Wrocław.

W ten sposób tworzymy środowisko organizacyjne, w którym każda przetwarzana informacja o kontrahencie, umowie, warunkach współpracy biznesowej, dane osobowe pracowników, współpracujących, uczestników inwestycji i innych osób, jak również innego rodzaju informacja posiadająca wartość gospodarczą podlega ochronie, a osoby bądź podmioty dokonujące naruszeń tej ochrony będą podlegały odpowiedzialności prawnej.

MINIMALIZACJA RYZYKA NARUSZENIA BEZPIECZEŃSTWA DANYCH

Nasze działania mają na celu minimalizować ryzyko naruszenia bezpieczeństwa informacji, w tym danych osobowych, dlatego wdrażamy środki zapobiegawcze, dzięki którym będzie to możliwe. Środki te przyjmują charakter techniczny, jak również fizyczny, organizacyjny oraz osobowy. Z uwagi na to, że informacje przetwarzają ludzie, dbamy o świadomość

naszych pracowników i współpracowników w zakresie ochrony danych, zapewniamy szkolenia, audyty oraz podejmujemy aktywne działania przy ryzyku naruszenia przetwarzanych informacji. Spełniamy także wymogi RODO dla przetwarzania danych osobowych, dbając o to, aby interes oraz prawa osób, których te dane dotyczą, nie zostały naruszone.

PRZYJMUJEMY POLITYKĘ BEZPIECZEŃSTWA INFORMACJI

Mając na uwadze powyższe, w celu zapewnienia bezpieczeństwa informacji, w tym danych osobowych, a także minimalizacji ryzyka naruszenia ochrony tych informacji, przyjmujemy niniejszą Politykę Bezpieczeństwa Informacji, a także zobowiązujemy wszystkie osoby zatrudnione i kierujące działalnością Miastoprojekt Wrocław, a także naszych kontrahentów do stosowania zasad w niej określonych.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

1. CEL

1.1. Celem niniejszej Polityki jest:

a. zapewnienie bezpieczeństwa informacji przetwarzanych w Miastoprojekt Wrocław;
b. zapewnienie ochrony danych osobowych przetwarzanych przez Miastoprojekt Wrocław, przede wszystkim w zakresie, w jakim Miastoprojekt Wrocław jest administratorem danych;
c. przeciwdziałanie naruszeniom bezpieczeństwa informacji, w tym naruszeniom ochrony danych osobowych;
d. podjęcie skutecznych działań w celu wykrywania oraz zapobiegania naruszeniom bezpieczeństwa informacji, w tym naruszeniom ochrony danych osobowych;
e. zwiększenie świadomości pracowników, współpracowników i kontrahentów Miastoprojekt Wrocław w zakresie bezpieczeństwa informacji, w tym ochrony danych osobowych.

2. ZAKRES

2.1. Niniejsza Polityka określa zasady przetwarzania informacji, w tym danych osobowych przez pracowników, współpracowników oraz kontrahentów Miastoprojekt Wrocław, a także zasady dotyczące zapewnienia bezpieczeństwa tych informacji oraz zasady postępowania w sytuacji naruszenia bezpieczeństwa informacji, w tym naruszenia

ochrony danych osobowych. Zasady te dotyczą przetwarzania jakichkolwiek informacji w systemach informatycznych Miastoprojekt Wrocław, dokumentach i materiałach w wersji papierowej Miastoprojekt Wrocław oraz informacji ujawnianych przez Miastoprojekt Wrocław kontrahentom.

2.2. Adresatami niniejszej Polityki są:

a. pracownicy i współpracownicy Miastoprojekt Wrocław;
b. kadra kierownicza Miastoprojekt Wrocław;
c. kontrahenci Miastoprojekt Wrocław, którym Miastoprojekt Wrocław przekazuje informacje, w tym dane osobowe, bądź którzy przetwarzają informacje dotyczące Miastoprojekt Wrocław.

3. DEFINICJE

administrator danych – podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych (w tym danych osobowych);

bezpieczeństwo informacji – zachowanie poufności, integralności i dostępności informacji, tj. stanu, w którym informacja nie jest ujawniana osobom nieupoważnionym, jest ona prawidłowa i kompletna, a także dostępna i użyteczna na żądanie upoważnionego personelu;

dane osobowe – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (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);

dostępność – właściwość zapewniająca, że osoby upoważnione będą miały dostęp do informacji tylko wtedy, gdy jest to uzasadnione;

informacja – każda informacja odnosząca się do kontrahenta Miastoprojekt Wrocław, umowy lub relacji biznesowej, której stroną jest Miastoprojekt Wrocław, w tym szczegóły takich umów oraz relacji biznesowych, danych osobowych przetwarzanych przez Miastoprojekt Wrocław lub tajemnicy przedsiębiorstwa Miastoprojekt Wrocław bądź innego podmiotu, a także inna informacja niejawna przetwarzana przez Miastoprojekt Wrocław w systemach informatycznych oraz dokumentacjach i materiałach w wersji papierowej;

integralność – właściwość zapewniająca, że informacja nie została zmieniona lub zniszczona w nieautoryzowany sposób;

kontrahent – osoba fizyczna lub prawa bądź jednostka organizacyjna nieposiadająca osobowości prawnej, której przepisy prawa zapewniają zdolność do czynności prawnych, będąca stroną umowy handlowej zawartej z Miastoprojekt Wrocław, a także pojawiająca się w inwestycjach, w których występuje Miastoprojekt Wrocław, jako uczestnik tych inwestycji;

Miastoprojekt Wrocław – Miastoprojekt Wrocław sp. z o.o. z siedzibą we Wrocławiu, ul. Snopkowa 2B, 52-225 Wrocław (KRS: 0000166714);

naruszenie bezpieczeństwa – każda sytuacja, która stwarza realne zagrożenie dla bezpieczeństwa informacji (np. atak hackerski, wykrycie złośliwego oprogramowania, utrata dokumentu, ujawnienie informacji osobie nieuprawnionej, wyciek danych);

Osoba Zaufania – osoba powoływana przez Zarząd do przyjmowania zgłoszeń nieprawidłowości oraz wyjaśniania wątpliwości związanych z postanowieniami niniejszej Polityki, powoływana zgodnie z postanowieniami Polityki zgłaszania nieprawidłowości, obowiązującej w Miastoprojekt Wrocław;

Polityka – niniejsza Polityka Bezpieczeństwa Informacji Miastoprojekt Wrocław sp. z o.o.;

poufność – właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom;

pracownik – osoba zatrudniona w Miastoprojekt Wrocław na podstawie umowy o pracę;

przełożony – osoba pełniąca funkcję bezpośredniego przełożonego pracownika lub współpracownika;

przetwarzanie informacji/ danych – operacja lub zestaw operacji wykonywanych na informacjach lub zestawach informacji w sposób zautomatyzowany lub niezautomatyzowany, tj. 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 informacji;

RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L Nr 119 z 2016 r.);

system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych (głównie: urządzenia

komputerowe, drukujące, łączności, oprogramowanie, sieć informatyczna i udostępniane przez nią zasoby);

współpracownik – osoba współpracująca z Miastoprojekt Wrocław na podstawie umowy cywilnoprawnej;

Zarząd – Zarząd Miastoprojekt Wrocław.

4. ZASADY POLITYKI BEZPIECZEŃSTWA INFORMACJI

4.1. Zgodność z prawem, zobowiązaniami i etyką

4.1.1. Zabronione jest przetwarzanie informacji niezgodnych z prawem, naruszeniem zobowiązań wynikających z umów, których stroną jest Miastoprojekt Wrocław, a także niezgodnych z zasadami etyki.

4.1.2. Miastoprojekt Wrocław sprawuje nadzór nad tym, aby przetwarzane przez niego informacje były przetwarzane zgodnie z prawem, zawartymi umowami i zasadami etycznymi.

4.2. Dostępność informacji

4.2.1. Wszelkie informacje mogą być przetwarzane wyłącznie przez osoby uprawnione do ich przetwarzania. Miastoprojekt Wrocław zapewnia tzw. ziarnistość informacji, co oznacza, że określona osoba ma dostęp wyłącznie do takich informacji, do jakich jest uprawniona.

4.2.2. Pracownicy i współpracownicy Miastoprojekt Wrocław uprawnieni są do przetwarzania informacji w zakresie i celach wynikających z ich obowiązków służbowych bądź umownych.

4.2.3. Kontrahenci Miastoprojekt Wrocław są uprawnieni do przetwarzania informacji przekazanych im przez Miastoprojekt Wrocław w zakresie i celach wynikających z realizowanej umowy zawartej z Miastoprojekt Wrocław.

4.3. Poufność informacji

4.3.1. Wszelkie informacje mają charakter poufny, za wyjątkiem informacji powszechnie dostępnych, tj. podanych do publicznej wiadomości w inny sposób niż poprzez naruszenie prawa lub zobowiązania umownego, którego dopuściła się jakakolwiek osoba.

4.3.2. Pracownicy, współpracownicy i kontrahenci Miastoprojekt Wrocław mają obowiązek zachowania poufności w stosunku do przetwarzanych przez nich informacji. Obowiązek zachowania poufności obowiązuje

pomimo ustania umów i relacji biznesowych z Miastoprojekt Wrocław, chyba że dana informacja utraciła wartość gospodarczą.

4.4. Integralność informacji

4.4.1. Niedopuszczalne jest przetwarzanie informacji w taki sposób, w którym istnieje ryzyko naruszenia ich integralności.

4.4.2. Miastoprojekt Wrocław stosuje takie środki bezpieczeństwa informacji, które uniemożliwiają osobie nieuprawnionej ingerencji w zakres oraz prawidłowość przetwarzanych informacji.

4.5. Niezbędność przetwarzania

4.5.1. Informacje powinny być przetwarzane wyłącznie w takim zakresie, w jakim jest to niezbędne dla osiągnięcia celów ich przetwarzania.

4.5.2. Nadmiarowe informacje powinny być usuwane bądź niepozyskiwane od osób lub podmiotów trzecich.

4.6. Informowanie o nieprawidłowościach

4.6.1. Pracownicy i współpracownicy Miastoprojekt Wrocław mają obowiązek informowania Miastoprojekt Wrocław o wszelkich nieprawidłowościach związanych z funkcjonowaniem systemu informatycznego, skutecznością stosowania środków zabezpieczających przetwarzane informacje, incydentami bezpieczeństwa informacji oraz wysokim ryzyku przetwarzania informacji.

4.6.2. Kontrahenci Miastoprojekt Wrocław mają obowiązek informowania Miastoprojekt Wrocław o wszelkich nieprawidłowościach związanych z funkcjonowaniem systemu DMS, jeśli mają do niego dostęp, incydentami bezpieczeństwa informacji dotyczących Miastoprojekt Wrocław lub jego pracowników bądź współpracowników, a także wysokim ryzyku przetwarzania informacji.

4.7. Warunki przetwarzania informacji

4.7.1. Informacje w formie papierowej przetwarzane są wyłącznie w warunkach, w jakich nie jest możliwe ich ujawnienie osobom lub podmiotom nieuprawnionym ani ich kradzież, ingerencja w ich treść czy zniszczenie, a także przy zastosowaniu środków bezpieczeństwa o charakterze fizycznym, organizacyjnym i osobowym, które

zapewniają bezpieczeństwo informacji adekwatne do występującego ryzyka.

4.7.2. Informacje w formie elektronicznej przy zastosowaniu systemu informatycznego przetwarzane są wyłącznie w warunkach, w jakich nie jest możliwe ich ujawnienie osobom lub podmiotom nieuprawnionym ani ich kradzież, wyciek, ingerencja w ich treść czy usunięcie, a także przy zastosowaniu środków bezpieczeństwa o charakterze technicznym, fizycznym, organizacyjnym i osobowym, które zapewniają bezpieczeństwo informacji adekwatne do występującego ryzyka, w szczególności środków uwierzytelniających dostęp do przetwarzanych informacji, umożliwiających przywrócenie utraconych informacji oraz zabezpieczających system informatyczny przed atakiem hackerskim, złośliwym oprogramowaniem oraz innymi szkodliwymi działaniami z zewnątrz.

4.7.3. Zabrania się przetwarzania informacji, gdy ryzyko naruszenia bezpieczeństwa informacji jest co najmniej wysokie. W takiej sytuacji należy wdrożyć środki minimalizujące występujące ryzyko, aby zapewnić wystarczające bezpieczeństwo informacji, jakie mają być przetwarzane. O wystąpieniu wysokiego ryzyka naruszenia bezpieczeństwa informacji należy niezwłocznie poinformować Miastoprojekt Wrocław.

4.8. Środki zabezpieczające

4.8.1. Miastoprojekt Wrocław zapewnia stosowanie środków bezpieczeństwa przetwarzanych informacji. Środki te zostały określone w pkt. 6.1 niniejszej Polityki.

4.8.2. Miastoprojekt Wrocław dokonuje analizy ryzyka naruszenia bezpieczeństwa informacji, a także podejmuje inne środki bezpieczeństwa informacji, które zostały określone w pkt. 6 niniejszej Polityki.

4.8.3. Kontrahenci Miastoprojekt Wrocław zobowiązani są do zapewnienia środków zabezpieczających informacje przekazywane im przez Miastoprojekt Wrocław albo dotyczące Miastoprojekt Wrocław lub jego pracowników bądź współpracowników, odpowiednie do poziomu ryzyka naruszenia bezpieczeństwa tych informacji oraz kategorii przetwarzanych informacji.

4.9. Obowiązki osób przetwarzających informacje

4.9.1. Każda osoba przetwarzająca informacje ma obowiązek:

a. zachowania tych informacji w poufności;
b. stosować wdrożone w jej przedsiębiorstwie środki bezpieczeństwa informacji;
c. dbać o bezpieczeństwo dokumentów, w szczególności nie zostawiać dokumentów bez nadzoru w godzinach pracy, przechowywać dokumenty w zamkniętych szafach lub biurkach po zakończeniu godzin pracy, niszczyć niepotrzebne dokumenty w niszczarce, nie pozostawiać dokumentów na drukarce, niezwłocznie usuwać wykonane skany oraz zabierać sporządzone kopie dokumentów;
d. wykorzystywać wyłącznie taką liczbę kopii dokumentów lub informacji, jaka jest niezbędna dla realizacji określonej czynności;
e. zabezpieczać dokumenty, urządzenia lub nośniki informacji przy przetwarzaniu informacji poza siedzibą przedsiębiorstwa, w szczególności na terenie budowy objętej realizowaną inwestycją.

4.9.2. Każda osoba przetwarzająca informacje w systemie informatycznym ma obowiązek:

a. zabezpieczać dostęp do swojego konta użytkownika w systemie informatycznym, w szczególności poprzez stosowanie poufnego hasła dostępu oraz blokowanie ekranu na czas nieobecności przy stanowisku pracy;
b. zapewnić bezpieczeństwo systemu informatycznego poprzez nieodczytywanie wiadomości e-mail pochodzących od nieznanych nadawców, niepobieranie nieznanej zawartości z e-maili oraz innych źródeł internetowych, a także nieinstalowanie programów (aplikacji) komputerowych bez nadzoru informatyka;
c. informować bezpośredniego przełożonego, informatyka lub Miastoprojekt Wrocław albo kontrahenta o incydentach bezpieczeństwa oraz nieprawidłowościach systemu informatycznego, które powodują ryzyko naruszenia bezpieczeństwa informacji;
d. korzystać z systemu informatycznego zgodnie z instrukcjami, regulaminami bądź innymi dokumentami wewnętrznymi, określającymi zasady korzystania z systemów informatycznych.

4.10. Zapewnienie właściwej obsługi informatycznej

4.10.1. Miastoprojekt Wrocław wyznacza Administratora Systemu Informatycznego, który sprawuje nadzór nad prawidłowością funkcjonowania systemów informatycznych Miastoprojekt Wrocław, zwłaszcza pod kątem bezpieczeństwa informacji przetwarzanych w tych systemach informatycznych.

4.10.2. Miastoprojekt Wrocław oczekuje, aby jego kontrahenci wyznaczyli w swoich przedsiębiorstwach administratora systemu informatycznego bądź podmiot zapewniający obsługę informatyczną ich systemów informatycznych, zwłaszcza pod kątem bezpieczeństwa informacji przetwarzanych w tych systemach informatycznych.

4.11. Zapobieganie i wykrywanie naruszeń bezpieczeństwa informacji

4.11.1. Za kluczowy element niniejszej Polityki Miastoprojekt Wrocław uznaje zapobieganie naruszeniom informacji. W tym celu Miastoprojekt Wrocław przeprowadza audyty, szkolenia oraz opracowuje analizę ryzyka, o których mowa w pkt. 6.2-6.4 niniejszej Polityki. Miastoprojekt Wrocław może podjąć również inne środki zapobiegawcze, jeżeli przyczyni się to do przeciwdziałania naruszeniom bezpieczeństwa informacji.

4.11.2. Miastoprojekt Wrocław stawia sobie za cel wykrywanie wszelkich naruszeń bezpieczeństwa informacji i w związku z tym określa procedurę postępowania w sytuacji naruszenia bezpieczeństwa informacji. Postanowienia tej procedury zostały określone w pkt. 6 niniejszej Polityki.

4.12. Zakaz ingerowania we właściwości systemu informatycznego

4.12.1. Pracownicy, współpracownicy oraz kontrahenci i osoby działające w imieniu kontrahentów Miastoprojekt Wrocław, którzy mają dostęp do system informatycznego Miastoprojekt Wrocław, mają bezwzględny zakaz ingerowania we właściwości takiego systemu informatycznego, w szczególności zakaz zmieniania konfiguracji ustawień, które nie są dostępne dla użytkownika takiego systemu informatycznego.

4.12.2. W sytuacji wykrycia możliwości ingerowania we właściwości systemu informatycznego przez użytkownika osoba, która wykryła taką możliwość, ma obowiązek niezwłocznie zawiadomić o tym Miastoprojekt Wrocław.

4.13. Przetwarzanie informacji poza siedzibą

4.13.1. Przetwarzanie informacji przez pracowników i współpracowników Miastoprojekt Wrocław poza jego siedzibą możliwe jest wyłącznie wtedy, jeśli jest to związane z czynnościami służbowymi bądź wykonywaniem umowy.

4.13.2. Przetwarzane informacji poza siedzibą przedsiębiorstwa stanowi szczególną sytuację przetwarzania informacji, która wymaga podjęcia wzmożonych środków bezpieczeństwa informacji. Pracownicy i współpracownicy przetwarzający informacje poza siedzibą Miastoprojekt Wrocław mają obowiązek zastosowania się do następujących zasad:

a. podczas transportu, przechowywania i wykorzystania nośników zawierających informacje (dokumenty, urządzenia, pendrive'y) pracownik lub współpracownik zachowa szczególną ostrożność pod kątem bezpieczeństwa informacji;
b. nośniki zawierające informacje nie będą pozostawiane bez nadzoru w miejscach powszechnie dostępnych;
c. pracownik lub współpracownik nie będzie korzystał z publicznych sieci internetowych, w tym publicznych sieci Wi-Fi;
d. pracownik lub współpracownik wykona polecenia lub instrukcje Miastoprojekt Wrocław w zakresie bezpieczeństw informacji.

4.14. Zapewnienie tajemnicy przedsiębiorstwa

4.14.1. Pracownicy i współpracownicy Miastoprojekt Wrocław mają obowiązek ze szczególną dbałością przetwarzać i zabezpieczać informacje stanowiące tajemnicę przedsiębiorstwa Miastoprojekt Wrocław, a także informacje stanowiące tajemnicę przedsiębiorstwa kontrahentów Miastoprojekt Wrocław.

4.14.2. Kontrahenci Miastoprojekt Wrocław mają obowiązek dołożyć najwyższych starań do przetwarzania i zabezpieczania informacji stanowiących tajemnicę przedsiębiorstwa Miastoprojekt Wrocław.

4.14.3. Informacje stanowiące tajemnicę przedsiębiorstwa Miastoprojekt Wrocław oraz kontrahentów Miastoprojekt Wrocław, a także szczególne zasady i procedury związane z ochroną tajemnicy przedsiębiorstwa zostały określone w Polityce Ochrony Własności Intelektualnej, obowiązującej w Miastoprojekt Wrocław.

5. OCHRONA DANYCH OSOBOWYCH

5.1. Miastoprojekt Wrocław zapewnia przetwarzanie danych osobowych w sposób zgodny z powszechnie obowiązującymi przepisami prawa w zakresie ochrony danych osobowych, w szczególności RODO, a także wewnętrzną Polityką Bezpieczeństwa Danych Osobowych, obowiązującą w Miastoprojekt Wrocław.

5.2. Miastoprojekt Wrocław zobowiązuje swoich pracowników i współpracowników do przetwarzania danych osobowych w sposób zgodny z RODO oraz na zasadach określonych w wewnętrznej Polityce Bezpieczeństwa Danych Osobowych, obowiązującej w Miastoprojekt Wrocław.

5.3. Miastoprojekt Wrocław zobowiązuje swoich kontrahentów do przetwarzania danych osobowych osób reprezentujących, pracowników i współpracowników Miastoprojekt Wrocław oraz innych osób, których dane zostaną przekazane kontrahentowi przez Miastoprojekt Wrocław, w sposób zgodny z powszechnie obowiązującymi przepisami prawa w zakresie ochrony danych osobowych, w szczególności RODO, w szczególności stosowania środków bezpieczeństwa, o których mowa w art. 32 RODO.

5.4. Miastoprojekt Wrocław wywiązuje się z ciążących na nim obowiązków prawnych określonych w RODO, w szczególności obowiązku informacyjnego dotyczącego przetwarzania danych osobowych, stosowania środków bezpieczeństwa przetwarzania danych osobowych, prowadzenia rejestrów, o których mowa w RODO, a także dopuszczania do przetwarzania danych osobowych wyłącznie osób upoważnionych.

5.5. Pracownicy, współpracownicy i kontrahenci Miastoprojekt Wrocław mają obowiązek przetwarzania danych osobowych z poszanowaniem następujących zasad:

a. *zasady zgodności z prawem, rzetelności i przejrzystości* – zgodnie z którą dane osobowe muszą być przetwarzane zgodnie z prawem, z uwzględnieniem interesów i rozsądnych oczekiwań osób, które dane dotyczą, uczciwie oraz przejrzyście, tj. przy poinformowaniu osoby, której dane dotyczą, o przetwarzaniu jej danych osobowych;
b. *zasady ograniczenia celu przetwarzania* – zgodnie z którą dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie

uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;

c. *zasady minimalizacji danych* – zgodnie z którą dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów ich przetwarzania;
d. *zasady prawidłowości* – zgodnie z którą dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane;
e. *zasady ograniczenia przechowywania* – zgodnie z którą dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, które dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
f. *zasady integralności i poufności* – zgodnie z którą dane osobowe muszą być 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.

5.6. Pracownicy, współpracownicy, kontrahenci oraz pracownicy kontrahenta mają obowiązek:

a. zachowania poufności w stosunku do przetwarzanych przez nich danych osobowych, niezależnie od dalszej współpracy z Miastoprojekt Wrocław (obowiązek zachowania poufności nieograniczony w czasie);
b. stosować wdrożone w ich przedsiębiorstwie środki bezpieczeństwa danych osobowych;
c. dbać o bezpieczeństwo dokumentów zawierających dane osobowe, w szczególności nie zostawiać dokumentów bez nadzoru w godzinach pracy, przechowywać dokumenty w zamkniętych szafach lub biurkach po zakończeniu godzin pracy oraz niszczyć niepotrzebne dokumenty w niszczarce;
d. zabezpieczać dostęp do swojego konta użytkownika w systemie informatycznym, w szczególności poprzez stosowanie poufnego hasła dostępu oraz blokowanie ekranu na czas nieobecności przy stanowisku pracy;
e. zapewnić bezpieczeństwo systemu informatycznego poprzez nieodczytywanie wiadomości e-mail pochodzących od nieznanych nadawców, niepobieranie nieznanej zawartości z e-maili oraz innych

źródeł internetowych, a także nieinstalowanie programów (aplikacji) komputerowych bez nadzoru informatyka;

f. dochowywać szczególnej staranności przy przetwarzaniu danych osobowych;
g. nie przesyłać zbiorów danych osobowych poprzez wiadomość e-mail bez szyfrowania tych zbiorów danych osobowych (np. poprzez spakowanie plików do formatu RAR i zabezpieczenie go hasłem dostępu);
h. informować bezpośredniego przełożonego, informatyka lub Miastoprojekt Wrocław albo kontrahenta o incydentach bezpieczeństwa oraz nieprawidłowościach systemu informatycznego, które powodują ryzyko naruszenia ochrony danych osobowych;
i. informować bezpośredniego przełożonego lub Miastoprojekt Wrocław albo kontrahenta o żądaniu realizacji określonych praw przez osobę, której dotyczą dane osobowe.

5.7. Kontrahenci Miastoprojekt Wrocław zobowiązują swoich pracowników oraz inne osoby, którymi posługują się przy realizacji swoich zobowiązań wobec Miastoprojekt Wrocław, do stosowania obowiązków określonych w pkt. 5.6 niniejszej Polityki. Za niespełnienie tych obowiązków przez personel Kontrahenta odpowiedzialność ponosi Kontrahent.

5.8. Miastoprojekt Wrocław nie ujawnia przetwarzanych danych osobowych osobom ani podmiotom trzecim, za wyjątkiem odbiorców tych danych. Odbiorcami danych są podmioty współpracujące z Miastoprojekt Wrocław przy realizacji celów przetwarzania. Najczęściej są to podmioty świadczące na rzecz Miastoprojekt Wrocław usługi: księgowe, informatyczne, prawne, podatkowe, audytorskie, inspekcji nadzoru, kurierskie i inne, jeśli w celu realizacji takich usług niezbędne jest przetwarzanie danych osobowych. Z podmiotami tymi Miastoprojekt Wrocław zawiera umowy powierzenia przetwarzania danych osobowych, spełniające wymagania określone w art. 28 RODO.

5.9. Miastoprojekt Wrocław uwzględnia ochronę danych osobowych w fazie projektowania (tzw. *privacy by design*), uwzględniając stan wiedzy technicznej, koszt wdrożenia lub udoskonalenia środków zabezpieczających przetwarzane dane osobowe oraz charakter, zakres, kontekst i cele przetwarzania, a ponadto ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, wynikające z przetwarzania.

5.10. Miastoprojekt Wrocław nie przekazuje danych osobowych do państw trzecich w rozumieniu RODO. W sytuacji zaistnienia konieczności przekazania danych osobowych do państw trzecich Miastoprojekt Wrocław dokona takiego przekazania danych wyłącznie w oparciu o przepisy RODO, przy zastosowaniu szczególnych środków ochrony danych osobowych.

5.11. Do zasad ochrony danych osobowych określonych powyżej stosuje się odpowiednio zasady określone w pkt. 4 niniejszej Polityki, chyba że z postanowień pkt. 5 niniejszej Polityki wynika co innego.

6. ŚRODKI BEZPIECZEŃSTWA

6.1. Miastoprojekt Wrocław zapewnia środki bezpieczeństwa przetwarzanych informacji, w tym danych osobowych, odpowiednie do poziomu ryzyka naruszenia bezpieczeństwa tych informacji oraz kategorii przetwarzanych informacji, do których należą:

a. środki ochrony fizycznej informacji, związane przede wszystkim z zabezpieczeniem dostępu do pomieszczeń, w których przetwarzane są informacje;
b. techniczne środki ochrony informacji, związane przede wszystkim z bezpieczeństwem systemów informatycznych;
c. osobowe środki ochrony informacji, związane z funkcjami pełnionymi przez określone osoby oraz obowiązkami i przeszkoleniem pracowników i współpracowników w zakresie bezpieczeństwa informacji, w tym ochrony danych osobowych;
d. środki organizacyjne ochrony informacji, związane z procedurami, zasadami i instrukcjami w zakresie bezpieczeństwa informacji, w tym ochrony danych osobowych;
e. inne środki zabezpieczenia informacji, wpływające na bezpieczeństwo przetwarzanych informacji, w tym ochronę danych osobowych.

6.2. Miastoprojekt Wrocław zapewnia swoim pracownikom i współpracownikom szkolenia z zakresu bezpieczeństwa informacji oraz ochrony danych osobowych, których celem jest zwiększenie świadomości w tym zakresie, utrwalenie poznanych zasad bezpieczeństwa informacji, w tym zasad ochrony danych osobowych, a także przygotowanie na wypadek ewentualnego naruszenia

bezpieczeństwa informacji, w tym naruszenia ochrony danych osobowych.

6.3. Szczegółowy opis środków bezpieczeństwa przetwarzanych informacji został określony w wewnętrznej dokumentacji Miastoprojekt Wrocław. Miastoprojekt Wrocław może podjąć inne środki bezpieczeństwa przetwarzanych informacji, jeśli przyczyni się to do zapobiegania naruszeniom bezpieczeństwa informacji lub minimalizacji ryzyka w tym obszarze.

6.4. Miastoprojekt Wrocław wymaga od swoich kontrahentów, aby dla przetwarzanych przez nich informacji dotyczących Miastoprojekt Wrocław lub związanych z realizacją umowy, których Miastoprojekt Wrocław jest stroną, a także dotyczących osób reprezentujących, pracowników lub współpracowników Miastoprojekt Wrocław, zapewnili odpowiednie lub zbliżone środki bezpieczeństwa, o których mowa w pkt. 6.1-6.4 niniejszej Polityki. Miastoprojekt Wrocław zastrzega sobie prawo do kontroli środków bezpieczeństwa stosowanych przez jego kontrahentów pod kątem ich adekwatności do ryzyka naruszenia bezpieczeństwa informacji, w tym ryzyka naruszenia ochrony danych osobowych.

7. POSTĘPOWANIE W SYTUACJI NARUSZENIA BEZPIECZEŃSTWA INFORMACJI

7.1. Każda osoba, która wykryje naruszenie bezpieczeństwa informacji, w tym naruszenie ochrony danych osobowych ma obowiązek:

a. poinformowania o nieprawidłowości swojego przełożonego;
b. poinformowania o nieprawidłowości Administratora Systemu Informatycznego, jeśli nieprawidłowość związana jest z funkcjonowaniem systemu informatycznego;
c. podjąć czynności niezbędne do powstrzymania skutków naruszenia (np. odłączyć komputer od zasilania, wyłączyć prąd, zamknąć pomieszczenie, usunąć dokument lub szkodliwy plik);
d. wstępnie ustalić okoliczności naruszenia oraz okoliczności wykrycia naruszenia (m.in. datę i czas, sposób wykrycia, zaobserwowany stan faktyczny).

7.2. W sytuacji gdy naruszenie dotyczy ochrony danych osobowych, a w przedsiębiorstwie powołany został inspektor ochrony danych,

bezpośredni przełożony osoby, która wykryła naruszenie, ma obowiązek niezwłocznie zawiadomić o tym inspektora ochrony danych.

7.3. Każda osoba, która podejrzewa, że mogło dojść do naruszenia bezpieczeństwa informacji, w tym naruszenia ochrony danych osobowych, albo posiada informacje dotyczące nieprawidłowości w zakresie bezpieczeństwa informacji lub przestrzegania postanowień niniejszej Polityki, ma obowiązek dokonać zgłoszenia nieprawidłowości na zasadach określonych w Polityce Zgłaszania Nieprawidłowości, obowiązującej w Miastoprojekt Wrocław.

7.4. Każde naruszenie odnotowywane jest w rejestrze nieprawidłowości, a naruszenie ochrony danych osobowych dodatkowo odnotowywane jest w rejestrze incydentów zagrażających bezpieczeństwu danych osobowych, prowadzonym przez administratora danych.

7.5. W zakresie dotyczącym naruszeń ochrony danych osobowych szczegółowe postanowienia proceduralne zostały określone w wewnętrznej Polityce Bezpieczeństwa Danych Osobowych, obowiązującej w Miastoprojekt Wrocław.

8. POSTANOWIENIA KOŃCOWE

8.1. Za realizację postanowień niniejszej Polityki odpowiada Zarząd. Zarząd może wyznaczyć osobę lub podmiot realizujący określone zadania wynikające z treści niniejszej Polityki.

8.2. W przypadku powstania jakichkolwiek wątpliwości co do treści niniejszej Polityki lub braku jej zrozumienia, osoby których to dotyczy mają obowiązek zwrócenia się do Zarządu lub Osoby Zaufania celem wyjaśnienia wątpliwości lub niezrozumiałej treści.

8.3. Naruszenie postanowień niniejszej Polityki stanowi ciężkie naruszenie obowiązków pracowniczych (w stosunku do pracowników) albo ważny powód uzasadniający rozwiązanie umowy (w stosunku do współpracowników).

8.4. Niniejsza Polityka obowiązuje od dnia jej przyjęcia przez Zarząd Miastoprojekt Wrocław do dnia jej wygaśnięcia albo zastąpienia nową treścią.

DOKUMENTY POWIĄZANE

- Polityka Zgłaszania Nieprawidłowości
- Polityka Ochrony Własności Intelektualnej
- Komunikat Prezesa Zarządu Miastoprojekt Wrocław Sp. z o.o. ws. powołania Osoby Zaufania
- Wewnętrzna Polityka Bezpieczeństwa Danych Osobowych (dokument niejawny)