Polityka Bezpieczeństwa Danych Osobowych

Terawat Dystrybucja Sp. z o.o.

Ul. Wrocławska 94

41-902 Bytom

KRS: 0000393933

NIP: 6263002689

REGON: 242709410

Obowiązująca od: 13.07.2026 r.

Sporządzona przez: ***Barbara Bzdziuch*** – *Inspektor Ochrony Danych*

Zatwierdzona przez: ***Tomasz Siulczyński*** – *Prezes Zarządu*

Rozdział I

Postanowienia ogólne

§ 1.

1. Polityka Bezpieczeństwa to zbiór zasad i procedur wraz z planem ich wdrożenia i egzekwowania, według których Terawat Dystrybucja Sp. z o. o. zarządza bezpieczeństwem danych osobowych. Prezentuje swoisty zbiór metod i zasad ochrony oraz zapewnia bezpieczeństwo danych osobowych, jako głównego zasobu spółki. Umożliwia ona zorganizowane i bezpieczne przetwarzanie informacji, sprawne i kontrolowane zarządzanie nimi, a także ochronę i ich bezpieczeństwo. Określa uprawnienia, obowiązki i odpowiedzialność osób uczestniczących w procesie przetwarzania danych osobowych.

2. Bezpieczeństwo danych osobowych to zachowanie poufności, integralności i dostępności danych z uwzględnieniem takich atrybutów jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Przy czym, przez poufność danych należy rozumieć zapewnienie, że dostęp do danych osobowych mają tylko osoby upoważnione, a przez dostępność danych, że osoby upoważnione mają dostęp do danych osobowych i związanych z nią aktywów wtedy gdy istnieje taka potrzeba, natomiast przez integralność danych rozumie się właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

3. Celem opracowania Polityki Bezpieczeństwa jest zdefiniowanie ogólnych wymagań oraz zasad ochrony danych osobowych, które będą fundamentem dla wszystkich dokumentów związanych z bezpieczeństwem danych osobowych.

4. Dokumenty związane z bezpieczeństwem danych powinny być przeglądane, aktualizowane w zależności od zmieniających się warunków i potrzeb. Przeglądów należy dokonywać, co najmniej raz w roku.

5. Wszystkie osoby zatrudnione w Terawat Dystrybucja Sp. z o. o., a także odbywające staż lub praktykę ponoszą odpowiedzialność za bezpieczeństwo danych, w ramach realizowanych przez siebie obowiązków.

6. Przetwarzanie danych osobowych jest dopuszczalne tylko pod warunkiem przestrzegania Rozporządzenia Parlamentu Europejskiego i Rady 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 ochrony danych) i wydanych na ich podstawie krajowych przepisów wykonawczych oraz opracowanych na ich podstawie procedur i regulaminów wprowadzonych w Terawat Dystrybucja Sp. z o. o.

7. Dane osobowe mogą być przetwarzane w postaci papierowej oraz przy użyciu systemów informatycznych.

Rozdział II

Postępowanie przy upoważnianiu osób do przetwarzania danych osobowych

§ 2.

1. Po przyjęciu do pracy/na staż/praktykę bezpośredni przełożony kieruje pracownika/stażystę/praktykanta do Inspektora Ochrony Danych Osobowych, w celu przeszkolenia z zakresu danych osobowych.

2. Każdy nowo zatrudniony pracownik lub osoba odbywająca staż/praktykę Terawat Dystrybucja Sp. z o. o. mający dostęp do przetwarzania ochrony danych osobowych, zobowiązany jest do zapoznania się z wewnętrznymi regulacjami z zakresu ochrony danych osobowych oraz do podpisania stosownego oświadczenia i przyjęcia zobowiązania do zachowania poufności.

3. Szkolenie, o którym mowa w ust. 1 powyżej, osoby rozpoczynające pracę, staż bądź praktyki w Terawat Dystrybucja Sp. z o. o., odbywają przed uzyskaniem upoważnienia do przetwarzania danych osobowych. Ponowne szkolenia z zakresu ochrony danych osobowych, Inspektor Ochrony Danych Osobowych przeprowadza w przypadku:
    1) zmiany przepisów związanych z ochroną danych osobowych lub w innym czasie, jeżeli Inspektor Ochrony Danych uzna to zasadne,
    2) pisemnego zgłoszenia pracownika na szkolenie przez jego bezpośredniego przełożonego,
    3) wystąpienia incydentu naruszenia przetwarzania danych osobowych.

4. Do przetwarzania danych osobowych mogą być dopuszczeni pracownicy posiadający pisemne upoważnienie do przetwarzania danych, nadane przez Administratora Danych Osobowych.

5. Z wnioskiem o upoważnienie pracownika do przetwarzania danych osobowych występuje jego bezpośredni przełożony.

6. Upoważnienie do przetwarzania danych osobowych przygotowuje Inspektor Ochrony Danych.

7. Upoważnienie wydawane na czas określony lub do czasu ustania stosunku pracy/stażu/praktyki lub do odwołania. Zawarcie kolejnej, dowolnego rodzaju umowy o pracę/stażu wiąże się z koniecznością przygotowania nowego upoważnienia.

8. Upoważnienie do przetwarzania danych osobowych sporządza się w 3 egzemplarzach:
    1) 1 egzemplarz dołączany jest do dokumentów kadrowych,
    2) 1 egzemplarz otrzymuje osoba upoważniona,
    3) 1 egzemplarz pozostaje w rejestrze prowadzonym przez Inspektora Ochrony Danych.

9. Bezpośredni przełożony pracownika jest zobowiązany do informowania Inspektora Ochrony Danych oraz Administratora Danych Osobowych o zakończeniu stażu/praktyki lub ustaniu stosunku pracy, w celu cofnięcia upoważnienia do przetwarzania danych osobowych i odebrania uprawnień do pracy w systemach informatycznych.

10. Niniejsze postępowanie w zakresie nadawania upoważnień do przetwarzania danych osobowych ma zastosowanie również w przypadku zmiany zakresu upoważnienia.

11. Upoważnienie do przetwarzania danych osobowych powinno być tożsame z zakresem obowiązków służbowych, uprawnień i odpowiedzialności pracownika.

12. W przypadku pracowników, którzy nie dokonują przetwarzania danych, a jedynie przebywają w obszarze przetwarzania danych wydawane jest na wniosek bezpośredniego przełożonego, upoważnienie do przebywania w obszarze przetwarzania danych osobowych.

Rozdział III

Zasady przetwarzania danych osobowych

§ 3.

1. Dane osobowe przetwarzane w Terawat Dystrybucja Sp. z o. o. mogą być pozyskiwane bezpośrednio od osób, które te dane dotyczą lub z innych źródeł, w granicach dozwolonych przepisami prawa.

2. Dane osobowe mogą być przetwarzane wyłączeni dla celów, dla jakich były zbierane.

3. Przetwarzanie danych może odbywać się tylko w takim zakresie, który pozwoli na zrealizowanie celu, do którego zostały zebrane. Zabrania się zbierania nadmiarowych danych osobowych.

4. Przetwarzane dane osobowe powinny być kompletne i aktualne, pochodzić z wiarygodnego źródła.

5. Przetwarzanie danych osobowych nie może odbyć się w czasie dłuższym niż jest to niezbędne do osiągnięcia celu przetwarzania danych. Po osiągnięciu celu przetrwaniania dane osobowy należy zniszczyć lub zanonimizować, chyb, że przepisy szczególne stanowią inaczej.

6. Dane osobowe muszą być przetwarzane w sposób zapewniający odpowiedni poziom ich bezpieczeństwa, w tym ochronę przez niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem, uszkodzeniem za pomocą adekwatnych środków technicznych i organizacyjnych.

Rozdział IV

Zasady przetwarzania danych osobowych w systemie informatycznym

§ 4.

1. Stanowiska komputerowe w pomieszczeniach, gdzie przebywać mogą osoby nieupoważnione do przetwarzania danych osobowych winny być umieszczone w sposób, który uniemożliwi takim osobą wgląd do tych danych.

2. Każdy użytkownik posiadający dostęp do systemy informatycznego, w którym przetwarzane są dane osobowe, musi poosiadać w tym systemie swój unikalny identyfikator oraz indywidualne hasło.

3. Niedozwolone jest wysłanie danych osobowych na prywatny adres e-mail.

4. Przenośne nośniki danych mogą służyć do przechowywania danych osobowych tylko w wyjątkowych sytuacjach i po zastosowaniu środków ochrony kryptograficznej.

Rozdział V

Zasada czystego biurka, czystego ekranu

§ 5.

1. Zasada czystego biurka:
    1) każdy pracownik/stażysta/praktykant:
        a) zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są mu potrzebne do wykonywanej w danym momencie pracy,
        b) powinien unikać pozostawiania dokumentów papierowych bez nadzoru,
        c) po zakończonej pracy zobowiązany jest do zabezpieczenia dokumentów w formie papierowej w zamykanej na klucz szafie,

d) w przypadku konieczności zniszczenia papierowych zawierających dane osobowe, zobowiązany jest do wyrzucenia ich do przeznaczonych w tym celu pojemników lub do niszczarki.

2) kierownik komórki organizacyjnej odpowiada za pozostawienie niezabezpieczonych dokumentów, będących w posiadaniu komórki organizacyjnej.

2. Zasada czystego ekrany:
   1) komputer służący do pracy z danymi musi mieć ustawiony, włączający się automatycznie po 15 minutach bezczynności użytkownika, wygaszacz ekranu.
      W przypadku wznowienia aktywności wygaszacz powinien być wyłączny jedynie po podaniu odpowiedniego hasła,
   2) monitor powinien być ustawiony w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane osobowe,
   3) pracownik przed wyjściem z pomieszczenia powinien zablokować komputer, włączając wygaszacz ekranu lub w przypadku dłuższej nieobecności najlepiej wylogować się z systemu.

Rozdział VI

Zadania Administratora Danych Osobowych

§ 6.

1. Niniejsza polityka ma zastosowanie do danych przetwarzanych przez Terawat Dystrybucja Sp. z o. o.

2. Administrator przetwarza dane osobowe z mocy prawa.

3. Do zadań Administratora Danych Osobowych należy:
   1) dochowanie szczególnej staranności przy przetwarzaniu danych osobowych,
      w celu ochrony interesów osób, których dane dotyczą,
   2) nadawanie upoważnień do przetwarzania danych osobowych,
   3) decydowanie o celach i zakresie przetwarzanie danych osobowych,
   4) wypełnienie obowiązku informacyjnego wobec osób, których dane dotyczą,

5) zapewnienie dostępu do danych, uzupełnianie, uaktualnianie, sprostowywanie danych, czasowe lub stałe ograniczenie przetwarzania kwestionowanych danych lub ich usunięcie z rejestrów, przenoszenie danych, gdy zażąda tego osoba, której dane są przetwarzane przez Administratora Danych Osobowych,
6) decydowanie o środkach technicznych i organizacyjnych, zapewniających ochronę przetwarzania danych osobowych,
7) informowania organu nadzorczego o przypadkach naruszenia ochrony danych osobowych,
8) kontrolowanie prowadzenia rejestrów czynności przetwarzania danych osobowych oraz rejestru kategorii przetwarzania danych osobowych,
9) zawieranie umów powierzenia przetwarzania danych osobowych.

4. Administrator Danych Osobowych wyznacza Inspektora Ochrony Danych Osobowych zwanego dalej IOS, który nadzoruje przetwarzanie danych osobowych na podstawie niniejszej Polityki Bezpieczeństwa.

Rozdział VII

Obowiązki i uprawnienia Inspektora Ochrony Danych

§ 7.

Do obowiązków Inspektora Ochrony Danych należy w szczególności:

1) zapewnienie przestrzegania przepisów o ochroni danych osobowych poprzez:
   a. opracowywanie dokumentacji opisującej sposób przetwarzania danych i środki zapewniające ochronę przetwarzanych danych osobowych oraz zasad w niej określonych,
   b. aktualizację dokumentacji, o której mowa w pkt 1) niniejszego paragrafu, w razie takiej konieczności, nie rzadziej jednak, niż raz na rok,
   c. zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych, w tym regulacji wewnętrznych,
2) prowadzenie rejestry czynności przetwarzania danych osobowych,
3) prowadzenie rejestru kategorii przetwarzania danych osobowych,
4) przygotowanie upoważnień do przetwarzania danych osobowych,

5) prowadzenie rejestru upoważnień do przetwarzania danych osobowych,
6) przygotowanie umów powierzenia przetwarzania danych osobowych,
7) prowadzenie rejestru umów powierzenia przetwarzania danych osobowych,
8) informowanie ADO o przypadkach naruszeń danych osobowych,
9) prowadzenie rejestru naruszeń,
10) zatwierdzanie wzorów dokumentów związanych z bezpieczeństwem danych osobowych przygotowanych w poszczególnych komórkach organizacyjnych,
11) udzielenie odpowiedzi na bieżące pytania i wątpliwości z zakresu ochrony danych osobowych,
12) współpraca z organem nadzorczym,
13) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych,
14) organizowanie lub prowadzenie szkoleń z zakresu ochrony danych osobowych, dla osób przetwarzających dane osobowe w Terawat Dystrybucja Sp. z o. o.
15) planowanie i zalecanie audytu w zakresie przetwarzania danych osobowych.

§ 8.

W celu realizacji powierzanych zadań Inspektor Ochrony Danych w Terawat Dystrybucja Sp. z o. o. ma prawo:

1) kontrolować komórki organizacyjne, w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe,
2) wydawać zlecenia Kierownikom komórek organizacyjnych w zakresie bezpieczeństwa ochrony danych osobowych,
3) wymagać od wszystkich pracowników wyjaśnień w sytuacji naruszenia bezpieczeństwa danych osobowych,
4) żądać informacji mających wpływ na przetwarzania danych osobowych w Terawat Dystrybucja Sp. z o. o.

Rozdział VIII

Odpowiedzialność osób na stanowiskach samodzielnych i kierowniczych

§ 9.

Osoby zajmujące samodzielne i kierownicze stanowiska zobowiązane są do:

1) stałego nadzoru i przestrzegania stosowania środków mających na celu zapewnienie bezpieczeństwa powierzanego zasobu, w ramach zadań realizowanych przez podległą komórkę organizacyjną,

2) zgłaszania Inspektorowi Ochrony Danych Osobowych planowanego rejestrowania nowych czynności przetwarzania danych osobowych oraz wnoszenia o zmiany w czynnościach już zarejestrowanych,

3) występowania do Inspektora Ochrony Danych z wnioskiem o nadanie lub cofniecie upoważnienia podległym pracownikom w zakresie dostępu do zasobu danych osobowych,

4) bieżącej weryfikacji uprawnień i upoważnień podlegających im pracowników pod kątem zgodności z powierzonymi im zakresami czynności,

5) występowania do Inspektora Ochrony Danych z wnioskiem o przygotowywanie umów powierzenia przetwarzania danych osobowych, jeżeli przetwarzanie danych powierzane jest innemu podmiotowi lub osobie na podstawie odrębnej umowy,

6) wyboru podmiotu przetwarzającego, który zapewni wystarczającą gwarancję wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie chroniło prawa osób, których dane dotyczą,

7) stałego monitorowania zidentyfikowanych ryzyk,

8) bieżącej aktualizacji rejestru ryzyka w przypadku zmiany ich oceny bądź stwierdzenia nowych ryzyk lub eliminacji dotychczasowych,

9) zgłaszania Inspektorowi Ochrony Danych i Administratorowi Danych Osobowych wszystkich przypadków naruszenia bezpieczeństwa informacji

lub też nienależytego zabezpieczenia przetwarzanych danych osobowych, zgodnie z procedurą zgłaszania naruszeń,

10) przetwarzania danych osobowych (w tym udostępniania) będących w zasobie podległej komórki organizacyjnej, zgodnie z obowiązującymi przepisami dotyczącymi ochrony danych osobowych,

11) informowania osób, których dane są przetwarzane o:
    a. danych Administratora Danych Osobowych (nazwa, siedziba, numer telefonu, adres e-mail),
    b. danych kontaktowych Inspektora Ochrony Danych (adres e-mail, adres korespondencyjny),
    c. celu zbierania danych osobowych,
    d. zakresie zbierania danych osobowych,
    e. udostępnieniu danych osobowych innym odbiorcom,
    f. przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej,
    g. okresie przechowywania danych osobowych,
    h. dobrowolności lub obowiązku podania danych osobowych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej,
    i. prawie wglądu do treści swoich danych oraz możliwości ich uzupełniania
    i sprostowania,
    j. prawie dostępu do swoich danych osobowych,
    k. prawie do usunięcia danych — prawo do „bycia zapomnianym",
    l. prawie do ograniczenia przetwarzania,
    m. prawie do przeniesienia danych,
    n. prawie do sprzeciwu wobec przetwarzania,
    o. prawie do wniesienia skargi do organu nadzorczego,
    p. zautomatyzowanym przetwarzaniu danych,
    q. źródle pozyskania danych, w przypadku zbierania danych osobowych nie bezpośrednio od osoby, której dane dotyczą,
    r. uzyskiwaniu zgody osób, których dane będą przetwarzane na zasadzie dobrowolności, zgodnie z procedurą realizacji praw osób,

12) zapewnienia odpowiedniej ochrony danych osobowych już na etapie projektowania aktów prawnych, umów, rozwiązań organizacyjnych i technologicznych itp., mających wpływ na przetwarzanie danych osobowych, w szczególności poprzez:

a. sprawdzenie, czy istnieją przesłanki prawne przetwarzania danych osobowych,
b. sprawdzenie, czy istnieją odpowiednie środki techniczne i organizacyjne, niezbędne do odpowiedniej ochrony danych osobowych,
c. jeżeli środki, o których mowa wyżej nie istnieją lub są niedostateczne, należy je stworzyć lub dostosować przed wdrożeniem nowych rozwiązań,
d. konsultacje z Inspektorem Ochrony Danych w celu otrzymania akceptacji uregulowań w zakresie nowych rozwiązań.

13) zgłaszania wzorów nowych formularzy, druków i wniosków stosowanych w podległej komórce organizacyjnej,

14) zapoznania się z obowiązującymi przepisami prawa dotyczącymi ochrony danych osobowych,

15) uczestnictwa w organizowanych szkoleniach i zapoznawania się z regulacjami dotyczącymi ochrony danych osobowych,

16) stosowania określonych w Urzędzie Gminy Świerklaniec procedur i środków przetwarzania,

17) przestrzegania procedur właściwego użytkowania systemów informatycznych, w których przetwarza się dane osobowe, w tym do nieujawniania innym użytkownikom swoich loginów i haseł,

18) zabezpieczenia danych osobowych przed ich utratą, uszkodzeniem lub zniszczeniem, zmianą lub udostępnieniem osobom nieupoważnionym,

19) przedkładania Inspektorowi Ochrony Danych propozycji rozwiązań, których celem jest poprawa zabezpieczenia przed naruszeniem ochrony danych osobowych.

Rozdział IX

Odpowiedzialność pracowników

§ 10.

Pracownicy Terawat Dystrybucja Sp. z o. o. zobowiązani są do:

1) stosowania środków mających na celu zapewnienie bezpieczeństwa przetwarzanych danych osobowych, w ramach realizowanych zadań,
2) posiadania aktualnego upoważnienia do przetwarzania danych osobowych,
3) przetwarzania danych, zgodnie z posiadanymi uprawnieniami,
4) zgłaszania bezpośredniemu przełożonemu, Inspektorowi Ochrony Danych oraz Administratorowi Danych Osobowych wszystkich przypadków naruszenia bezpieczeństwa informacji lub też nienależytego zabezpieczenia przetwarzanych danych osobowych, zgodnie z procedurą zgłaszania naruszeń,
5) przetwarzania danych osobowych (w tym udostępniania) będących w zasobie podległej komórki organizacyjnej, zgodnie z obowiązującymi przepisami dotyczącymi ochrony danych osobowych,
6) informowania osób, których dane są przetwarzane o informacjach wskazanych
   w Rozdziale VIII §9 pkt 11 niniejszej Polityki Bezpieczeństwa,
7) zapoznania się z obowiązującymi przepisami prawa dotyczącymi ochrony danych osobowych,
8) uczestnictwa w organizowanych szkoleniach i zapoznawania się z regulacjami dotyczącymi ochrony danych osobowych,
9) stosowania określonych w Urzędzie Gminy Świerklaniec procedur i środków przetwarzania,
10) przestrzegania procedur właściwego użytkowania systemów informatycznych,
    w których przetwarza się dane osobowe, w tym do nieujawniania innym użytkownikom swoich loginów i haseł,
11) zabezpieczenia danych osobowych przed ich utratą, uszkodzeniem lub zniszczeniem, zmianą lub udostępnieniem osobom nieupoważnionym.

Rozdział X

Odpowiedzialność karna, cywilna i dyscyplinarna

§ 11.

Naruszenie przepisów o ochronie danych osobowych, może skutkować:

1) odpowiedzialnością dyscyplinarną na podstawie przepisów prawa pracy,
2) odpowiedzialnością karną za ujawnienie tajemnicy służbowej i zawodowej na podstawie przepisów prawa karnego,
3) odpowiedzialnością cywilną na podstawie przepisów prawa cywilnego.

Rozdział XI

Postanowienia końcowe

§ 12.

1. Osoba, która w przypadku powzięcia informacji o naruszeniu zasad bezpieczeństwa informacji lub w sytuacji uzasadnionego domniemania takiego naruszenia nie podjęta działania określonego w Polityce, może podlegać odpowiedzialności wynikającej z przepisów prawa.

2. Szczególnej ochronie podlegają informacje kancelarii tajnej. Sposób postępowania dokumentami kancelarii tajnej regulują odrębne przepisy.

§ 13.

Integralną część Polityki Bezpieczeństwa stanowią załączniki:

1) Rejestr czynności przetwarzanych danych osobowych – załącznik nr 1,
2) Procedura analizy ryzyka przetwarzania danych osobowych – załącznik nr 2,
3) Analiza ryzyka przetwarzania danych osobowych – załącznik nr 2a,
4) Procedura nadawania uprawnień w KSeF- załącznik nr 3,
5) Wzór upoważnienia do KSeF – załącznik nr 3a,
6) Rejestr uprawnień do KSeF - załącznik nr 3b,
7) Procedura ochrony danych osobowych w pracy zdalnej – załącznik nr 4,

8) Procedura zgłaszania naruszeń danych osobowych – załącznik nr 5,
9) Raport naruszenia danych osobowych – załącznik nr 5a,
10) Wzór ogólnego upoważnienia do przetwarzania danych osobowych – załącznik nr 6,
11) Wzór upoważnienia od przebywania w obszarze przetwarzania danych osobowych – załącznik nr 7,
12) Wzór wniosku o nadanie upoważnienia do przetwarzania danych osobowych – załącznik nr 8,
13) Wzór oświadczenia pracownika o zaufaniu poufności.
14) Wzór umowy na przetwarzanie danych osobowych – załącznik nr 10,
15) Wzór wniosku o przygotowanie umowy na przetwarzanie danych osobowych – załącznik nr 11.