Polityka Bezpieczeństwa Danych Osobowych w Grupie T4B

Spis treści

1. Wstęp

Zarząd T4B Sp z o.o. i zarządy pozostałych spółek należących do grupy przedsiębiorstw w skład której wchodzą:

- T4B SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ z siedzibą w Warszawie, Aleja Stanów Zjednoczonych 32/U15, 04 – 036 Warszawa KRS: 0000166640; NIP: 5262709541; REGON: 015503732 (**Główna Jednostka Organizacyjna Grupy T4B**);

- IPP SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ z siedzibą w Warszawie, Aleja Stanów Zjednoczonych 32/U15, 04 – 036 Warszawa, KRS: 0000168495; NIP: 5262709819; REGON: 015512820;

- T4B BUDOWNICTWO SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ z siedzibą w Warszawie, Aleja Stanów Zjednoczonych 32/U15, 04 – 036 Warszawa, KRS: 0000565357; NIP: 1132892450; REGON: 361961889;

- T4B EKOTECHNOLOGIE SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ z siedziba w Warszawie, Aleja Stanów Zjednoczonych 32/U15, 04 – 036 Warszawa, KRS: 0000502072; NIP: 5311690400; REGON: 147144564;

- SORT - BET SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ z siedziba w Warszawie, Aleja Stanów Zjednoczonych 32/U15, 04 – 036 Warszawa, KRS: 0000542298; NIP: 9161394500; REGON: 360753947,

- T-MASTER SPÓŁKA Z OGRANIOCZONĄ ODPOWIEDZIALNOŚCIĄ z siedzibą w Warszawie, Aleja Stanów Zjednoczonych 32/U15, 04 – 036 Warszawa, KRS: 0000696905; NIP: 5482686658; REGON: 368349766,

zwanymi dalej **Grupa Przedsiębiorstw T4B**, co odnosi się do każdego z w/w podmiotów osobno, jak też do wszystkich podmiotów jako całej grupy przedsiębiorstw,

mając na względzie powszechnie obowiązujące przepisy w zakresie ochrony danych osobowych, będąc świadome wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych powierzających spółkom z Grupy Przedsiębiorstw T4B swoje dane osobowe, deklarują:

- podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem danych osobowych;

- zapewnienia niezbędnych środków technicznych i organizacyjnych w celu utrzymywania ochrony danych osobowych na poziomie wymaganym przez obowiązujące w Rzeczpospolitej Polskiej prawo oraz w zgodzie z najlepszymi praktykami w tym zakresie;

- stałe podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w Grupie Przedsiębiorstw T4B w zakresie problematyki bezpieczeństwa tych danych;

- traktowania obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania przez zatrudnione osoby;

- podejmowania w niezbędnym zakresie współpracy z instytucjami powołanymi do ochrony danych osobowych.

Zarządy Spółek Grupy Przedsiębiorstw T4B są świadome zagrożeń związanych z przetwarzaniem przez Spółki danych osobowych, w tym w szczególności z zagrożeń wynikających z dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach teleinformatycznych. Zarządy spółek Grupy Przedsiębiorstw T4B deklarują, że będą stale doskonaliły i rozwijały organizacyjne, techniczne oraz informatyczne środki ochrony danych osobowych przetwarzanych zarówno metodami tradycyjnymi jak i elektronicznie tak, aby skutecznie zapobiegać zagrożeniom.

2. Cel i zakres dokumentu

Celem niniejszego dokumentu jest:

1.1. Określenie jednolitych standardów ochrony danych osobowych w Grupie Przedsiębiorstw T4B

1.2. Zapewnienie zgodności z przepisami prawa mającymi zastosowanie w obszarze ochrony danych osobowych. Ponadto dokument określa uprawnienia, odpowiedzialności i obowiązki pracowników w Grupie Przedsiębiorstw T4B w przedmiotowym obszarze.

3. Definicje

Na potrzeby niniejszego dokumenty wykorzystuje się poniższe pojęcia i definicje:

3.1. Administrator Systemu Teleinformatycznego (AST) – odpowiedzialny za bieżącą bezpieczną i efektywną eksploatację oraz rozwój zasobów teleinformatycznych spółek Grupy Przedsiębiorstw T4B leżących w obszarze jego odpowiedzialności, w tym systemy przetwarzania danych osobowych, zgodnie z najlepszymi praktykami i standardami. AST odpowiedzialny jest za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach.

3.2. Administrator Danych Osobowych (ADO) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

3.3. Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka

specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań;

3.4. **Inspektor Ochrony Danych (IOD)** – wyznaczona (powołana przez ADO) osoba monitorująca wypełnienie mających zastosowanie obowiązków wynikających z regulacji prawnych w obszarze danych osobowych w Spółce;

3.5. **Kategoria osób, których dane dotyczą** – kategoria / grupa osób, których dane osobowe są przetwarzane w T4B (m.in. pracownicy, właściciele nieruchomości, kontrahenci);

3.6. **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. Każde naruszenie ochrony danych osobowych traktowane jest jak incydent bezpieczeństwa informacji;

3.7. **Obowiązek informacyjny** – zakres informacji przekazywany osobie, której dane osobowe przetwarzane są przez Administratora Danych Osobowych zgodnie z art. 13 i 14 RODO;

3.8. **Odbiorca** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem Państwa Członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne powinno być zgodne z przepisami o ochronie danych osobowych mającymi zastosowanie stosownie do celów przetwarzania;

3.9. **Organ nadzorczy** - oznacza niezależny organ publiczny ustanowiony przez Państwo Członkowskie zgodnie z art. 51 RODO;

3.10. **Państwo trzecie** – Państwo, które nie wchodzi w skład EOG (Europejskiego Obszaru Gospodarczego);

3.11. **Podmiot przetwarzający** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu ADO;

3.12. **Podmiot zewnętrzny** – to osoba fizyczna, jednostka organizacyjna nieposiadająca osobowości prawnej lub osoba prawna z siedzibą w Polsce lub za granicą, organ administracji publicznej, oraz inne podmioty wykonujące zadania na rzecz Spółki;

3.13. **Pracownik** - to osoba zatrudniona w T4B. na podstawie umowy o pracę;

3.14. **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;

3.15. **Przedstawiciel** - oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii Europejskiej, która została wyznaczona na piśmie przez ADO lub podmiot przetwarzający na mocy art. 27 RODO do reprezentowania ADO lub podmiotu przetwarzającego w zakresie ich obowiązków;

3.16. **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;

3.17. **Pseudonimizacja** - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było 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;

3.18. **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;

3.19. **Spółka lub T4B**– T4B SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ z siedzibą w Warszawie, Aleja Stanów Zjednoczonych 32/U15, 04 – 036 Warszawa (**Główna Jednostka Organizacyjna Grupy T4B**);

3.20. **system teleinformatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;

3.21. **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.

4. Podstawy prawne ochrony danych osobowych w Grupie T4B.

4.1. Podstawę prawną zasad określonych w niniejszym dokumencie stanowi 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 oraz Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych /Dz. U. z 2018 r., poz. 1000

4.2. T4B jako Administrator Danych Osobowych deklaruje, że przetwarzanie danych osobowych w Spółce jest zgodne z mającymi zastosowanie wymaganiami prawnymi.

4.3. Deklaracja ta opiera się w szczególności na zapewnieniu, że dane osobowe są:

4.3.1. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,

4.3.2. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i przetwarzane w sposób zgodny z tymi celami,

4.3.3. adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,

4.3.4. prawidłowe i w razie potrzeby uaktualniane,

4.3.5. 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,

4.3.6. 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.

5. Podział obowiązków w zakresie ochrony danych osobowych w Spółce

5.1. Administrator Danych Osobowych jest odpowiedzialny za:

5.1.1. wprowadzenie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych w organizacji danych osobowych,

5.1.2. dostarczenie niezbędnych zasobów do zapewnienia zgodności z mającymi zastosowanie wymaganiami prawnymi w obszarze ochrony danych osobowych,

5.1.3. powoływanie i odwoływanie IOD oraz wspieranie IOD w wypełnianiu przez niego zadań,

5.1.4. zapewnienie kwalifikacji IOD, a w szczególności fachowej wiedzy nt. prawa i praktyk w dziedzinie ochrony danych osobowych.

5.2. Administrator Systemu Teleinformatycznego jest odpowiedzialny za:

5.2.1. nadzór nad infrastrukturą informatyczną Spółki oraz, w porozumieniu z IOD, podejmowanie decyzji o formach i metodach zabezpieczenia danych osobowych przetwarzanych w sieciach i systemach informatycznych Spółki,

5.2.2. administrację środowiskami informatycznymi przeznaczonymi do przetwarzania danych osobowych,

5.2.3. administrację uprawnieniami nadawanymi / modyfikowanymi / odbieranymi do systemów informatycznych przetwarzających dane osobowe,

5.2.4. zapewnienie ciągłości działania systemu informatycznego i optymalizację jego wydajności,

5.2.5. instalację i konfigurację sprzętu i oprogramowania,

5.2.6. konfigurację i administrację oprogramowaniem systemowym i sieciowym,

5.2.7. identyfikowanie i zgłaszanie do IOD ewentualnych problemów z zakresu bezpieczeństwa i ochrony danych osobowych,

5.2.8. zapewnienie bezpieczeństwa przechowywanych w systemie informatycznym danych osobowych.

5.2.9. przygotowanie i aktualizację wewnętrznych aktów prawnych dotyczących nadawania, zmiany i odbierania uprawnień dostępu do systemów informatycznych, służących do przetwarzania danych osobowych.

5.3. Inspektor Ochrony Danych Osobowych (IOD) jest odpowiedzialny za:

5.3.1. nadzorowanie opracowania, tworzenie i aktualizację wewnętrznych aktów prawnych (niniejszy dokument, procedury, instrukcje, regulaminy i inne dokumenty) dotyczących ochrony danych osobowych oraz nadzór nad ich przestrzeganiem,

5.3.2. prowadzenie dokumentacji przetwarzania danych osobowych wymaganych przez mające zastosowanie regulacje prawne,

5.3.3. prowadzenie i aktualizację Rejestru czynności przetwarzania danych osobowych,

5.3.4. kontakty z właściwym organem administracji publicznej ds. ochrony danych osobowych związane ze składaniem wyjaśnień oraz współpracę w przypadku kontroli przeprowadzanej przez inspektorów organu nadzorczego,

5.3.5. prowadzenie szkoleń w zakresie ochrony danych osobowych oraz zapewnienie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,

5.3.6. planowanie i nadzór nad audytami bezpieczeństwa zasobów informacyjnych T4B zawierających dane osobowe oraz raportowanie Zarządowi Spółki o ich wynikach i niezbędnych przedsięwzięciach podnoszących poziom bezpieczeństwa danych,

5.3.7. przeprowadzanie weryfikacji zgodności przetwarzania danych osobowych z mającymi zastosowanie regulacjami prawnymi w obszarze ochrony danych osobowych na żądanie organu nadzorczego lub ADO,

5.3.8. konsultowanie merytoryczne umów powierzenia przetwarzania danych osobowych,

5.3.9. nadzór nad realizacją oraz raportowanie wyników analizy ryzyka do ADO,

5.3.10. współpracę z Działem DevOps w zakresie nadzorowania pracy AST, opiniowania polityki zakupowej systemów informatycznych służących do przetwarzania danych osobowych i zapewnienia optymalnego poziomu bezpieczeństwa w sieciach i systemach informatycznych T4B służących do przetwarzania danych osobowych,

5.3.11. reagowanie na zgłoszone incydenty (w tym naruszenia ochrony danych osobowych),

5.3.12. opiniowanie wniosków o wdrożenie systemów informatycznych, w których przetwarzane są dane osobowe,

5.3.13. wydawanie opinii dotyczących zasad przetwarzania danych osobowych w T4B,

5.3.14. inicjowanie działań zwiększających poziom bezpieczeństwa danych osobowych w Spółce oraz koordynację działań związanych z programem podnoszenia poziomu wiedzy pracowników T4B z zakresu ochrony danych osobowych, w tym organizację szkoleń w zakresie ochrony danych osobowych.

5.4. Wszystkie osoby przetwarzające dane osobowe w T4B są odpowiedzialne za:

5.4.1. przestrzeganie zasad ochrony danych osobowych określonych w niniejszym dokumencie oraz dokumentach z nim związanych. W tym celu każdy użytkownik zobowiązany jest zapoznać się przed dopuszczeniem do przetwarzania danych z dokumentacją z zakresu ochrony danych osobowych oraz złożyć stosowne oświadczenie w formie zobowiązania pracownika do zachowania poufności danych osobowych, potwierdzające znajomość ich treści,

5.4.2. spełnianie wymogu wynikającego z obowiązku informacyjnego, w szczególności poinformowania osoby, której dane dotyczą zgodnie z zakresem wskazanym w niniejszym dokumencie,

5.4.3. uczestniczenie w obowiązkowym szkoleniu z zakresu ochrony danych osobowych,

5.4.4. bezzwłoczne zgłaszanie wszelkich dostrzeżonych nieprawidłowości w działaniu systemu informatycznego, w którym przetwarzane są dane osobowe zgodnie z zasadami zgłaszania incydentów w Spółce,

5.4.5. bezzwłoczne zgłaszanie wszelkich naruszeń, nieprawidłowości i dostrzeżonych zagrożeń związanych z bezpieczeństwem danych osobowych,

5.4.6. wnioskowanie do IOD o potrzebie uzupełnienia lub uaktualnienia Rejestru czynności przetwarzania danych osobowych, potrzebie dokonania zmian w procesie przetwarzania danych osobowych oraz informowanie o ustaniu celu przetwarzania tych danych,

5.4.7. niezwłoczne usunięcie / zaprzestanie przetwarzania danych osobowych w momencie ustania celu ich przetwarzania,

5.4.8. informowanie IOD o zamiarze powierzenia przetwarzania danych osobowych lub ich udostępnienia innemu podmiotowi oraz konsultowanie z IOD umowy o powierzeniu przetwarzania danych osobowych,

5.4.9. dołożenia szczególnej staranności podczas przetwarzania danych osobowych, aby proces przetwarzania odbywał się zgodnie z prawem, dane osobowe były merytorycznie poprawne, a ich przetwarzanie odbywało się wyłącznie w celu i zakresie oraz przez okres, dla którego zostały zebrane,

5.4.10. udzielanie wyjaśnień w zakresie dotyczącym przetwarzania przez nich danych osobowych na każdorazowe żądanie IOD.

6. Rejestr czynności przetwarzania danych osobowych

6.1. Dla wszystkich zidentyfikowanych kategorii danych osobowych, IOD przy współpracy z AST prowadzi Rejestr czynności przetwarzania danych osobowych.

6.2. Na rejestr czynności przetwarzania danych osobowych składają się co najmniej następujące pola:

a) opis kategorii osób, których dane dotyczą,
b) cel przetwarzania danych osobowych,
c) podstawa prawna przetwarzania,
d) źródło danych osobowych,
e) opis kategorii danych osobowych,

f) informacja o przetwarzaniu danych wrażliwych,
g) lokalizacje, w których przetwarzane są dane osobowe,
h) systemy informatyczne, w których przetwarzane są dane osobowe,
i) informacja o przetwarzaniu danych osobowych w formie papierowej,
j) planowany termin usunięcia danych osobowych,
k) stosowane zabezpieczenia organizacyjne i techniczne,
l) informacje o podmiotach, którym dokonano powierzenia i dalszego powierzenia danych osobowych,
m) informacje o podmiotach, którym udostępniono dane osobowe,
n) informacje o przekazaniu danych osobowych do Państwa trzeciego,
o) dane kontaktowe ADO oraz IOD.

6.3. Rejestr czynności przetwarzania danych osobowych może być prowadzony w formie papierowej, elektronicznej lub w systemie informatycznym.

6.4. Rejestr czynności przetwarzania stanowi załącznik nr 1 do niniejszej Polityki.

7. Środki techniczne i organizacyjne ochrony danych osobowych

7.1. W celu zapewnienia ochrony danych osobowych przetwarzanych w Spółce stosuje się następujące zabezpieczenia organizacyjne i techniczne:

7.1.1. opracowano i wdrożono „Zasady postępowania użytkownika zasobów teleinformatycznych w Grupie Przedsiębiorstw T4B".

7.1.2. regularnie przeprowadza się analizę ryzyka utraty bezpieczeństwa danych osobowych, a na podstawie jej wyników podejmuje się adekwatne działania zapewniające właściwy poziom bezpieczeństwa przetwarzanych danych osobowych,

7.1.3. do przetwarzania danych osobowych dopuszcza się wyłącznie osoby posiadające ważne upoważnienia do ich przetwarzania w zakresie niezbędnym do realizacji obowiązków służbowych,

7.1.4. zapewnia się realizację szkoleń dla wszystkich pracowników dopuszczonych do przetwarzania danych osobowych obejmujących zasady ich ochrony,

7.1.5. do przetwarzania danych osobowych dopuszcza się jedynie pracowników, którzy uprzednio pisemnie zobowiązali się do zachowania ich w poufności,

7.1.6. przetwarzania danych osobowych dokonuje się w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych, w szczególności poprzez: kontrolę dostępu do pomieszczeń i budynków, instalację alarmową, zapewnienie środków przetwarzania danych osobowych z trwałym znaczeniem otwarcia, w których przetwarza się dane osobowe (szafy, biurka zamykane na klucz),

7.1.7. każdą osobę przetwarzającą dane osobowe zobowiązuje się do przestrzegania zasad bezpieczeństwa informacji określonych w dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji,

7.1.8. przebywanie osób nieupoważnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe dopuszcza się tylko w obecności osoby upoważnionej do przetwarzania danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych,

7.1.9. stosuje się pisemne umowy powierzenia przetwarzania danych osobowych przy współpracy z podmiotami zewnętrznymi przetwarzającymi dane osobowe,
7.1.10. przetwarzanie danych osobowych odbywa się wyłącznie w ramach wykonywanych zadań służbowych,
7.1.11. zapewnia się zdolność do szybkiego przywrócenia dostępności danych osobowych w razie incydentu fizycznego lub technicznego,
7.1.12. zapewnia się zdolność do ciągłego zapewnienia poufności, integralności i dostępności danych osobowych przetwarzanych w systemach informatycznych Grupy PrzedsiębiorstwT4B,
7.1.13. dokonuje się regularnych audytów i testów skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych,
7.1.14. zapewnia się zdolność systemów informatycznych do spełnienia praw osób, których dane dotyczą (usunięcie, sprostowanie, sprzeciw, ograniczenie),
7.1.15. zapewnia się stosowanie środków ochrony informacji wynikających z wdrożonego w Spółce Systemu Zarządzania Bezpieczeństwem Informacji.

8. Realizacja obowiązku informacyjnego

8.1. Każdorazowo, podczas zbierania danych osobowych, należy przekazać osobie, której dane dotyczą:

8.1.1. tożsamość i dane kontaktowe ADO,
8.1.2. dane kontaktowe IOD,
8.1.3. cele przetwarzania danych osobowych oraz podstawę przetwarzania,
8.1.4. informacje, że przetwarzanie wykonywane jest do celów wynikających z uzasadnionych interesów realizowanych przez ADO,
8.1.5. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeśli istnieją,
8.1.6. gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz wzmiankę o stosowanych zabezpieczeniach, możliwościach uzyskania kopii tych danych lub o miejscu ich udostępnienia,
8.1.7. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
8.1.8. informacje o prawie do żądania od Spółki 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,
8.1.9. jeżeli przetwarzanie odbywa się na podstawie uzyskanej zgody - informacje o prawie do cofnięcia zgody na przetwarzanie danych osobowych,
8.1.10. informację o prawie do wniesienia skargi do organu nadzorczego,
8.1.11. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, istotnych zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

8.2. W przypadku, gdy dane osobowe zbierane są bezpośrednio od osoby, której dane dotyczą, należy przekazać 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 konsekwencjach niepodania danych.

8.3. W przypadku, gdy dane osobowe pozyskiwane są w inny sposób niż od osoby, której dane dotyczą, należy przekazać osobie, której dane dotyczą informacje zawarte w pkt. 7.1. uzupełnione o:

8.3.1. kategorie przetwarzanych danych osobowych,
8.3.2. źródło pochodzenia danych osobowych, a gdy ma to zastosowanie również informację, czy pochodzą one ze źródeł publicznie dostępnych.

8.4. W przypadku, gdy planuje się dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, należy poinformować osobę, której dane dotyczą, o nowym celu przetwarzania oraz udzielić jej stosowanych informacji zawartych w niniejszym punkcie.

8.5. Do realizacji obowiązku informacyjnego zobowiązani są wszyscy pracownicy Grupy Przedsiębiorstw T4B.

8.6. Obowiązek informacyjny w Grupie Przedsiębiorstw T4B należy realizować:

8.6.1. ustnie – w przypadku bezpośredniego kontaktu z osobą, której dane dotyczą,
8.6.2. pisemnie – jako integralną część umowy lub innego dokumentu z podmiotem zewnętrznym zawierającego dane osobowe lub jako osobny dokument.
8.6.3. w formie elektronicznej – jako informacja w systemie informatycznym przetwarzającym dane osobowe,
8.6.4. w formie e-mail – w przypadku korespondencji e-mail.

8.7. Podstawowe informacje wymagane mającymi zastosowanie regulacjami prawnymi w obszarze ochrony danych osobowych udostępniane są na stronie internetowej T4B.

8.8. Informacje zawarte w niniejszym rozdziale nie musza być przekazane osobie, której dane dotyczą w przypadku, gdy osoba ta, dysponuje już tymi informacjami – obowiązek informacyjny został spełniony w przeszłości.

9. Prawa osób, których dane przetwarzane są przez Grupę Przedsiębiorstw T4B

9.1. Prawo dostępu przysługujące osobie, której dane dotyczą:

9.1.1. Każda osoba, której dane dotyczą jest uprawniona do uzyskania potwierdzenia, czy w Spółce przetwarzane są jej dane osobowe.
9.1.2. Na wniosek osoby, której dane dotyczą, należy przekazać informację o:
9.1.2.1. celu przetwarzania danych osobowych,
9.1.2.2. kategoriach przetwarzanych danych osobowych,
9.1.2.3. odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w Państwach trzecich

lub organizacjach międzynarodowych oraz zabezpieczeniach wykorzystywanych w związku z tym przekazaniem,

9.1.2.4. okresie przechowywania danych osobowych, a gdy nie jest to możliwe, kryteriach tego okresu,

9.1.2.5. prawie do żądania od ADO sprostowania, usunięcia lub ograniczenia przetwarzania jej danych osobowych, oraz prawie wniesienia sprzeciwu wobec takiego przetwarzania,

9.1.2.6. prawie wniesienia skargi do organu nadzorczego,

9.1.2.7. źródle pozyskiwania danych osobowych, jeśli nie zostały zebrane od osoby, której dane dotyczą,

9.1.2.8. zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, istotnych zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

9.1.3. W przypadku wystąpienia przez osobę, której dane dotyczą o kopię danych osobowych, należy zgłosić taki fakt IOD.

9.1.4. IOD, po weryfikacji tożsamości osoby wnioskującej, dostarcza kopię danych podlegających przetwarzaniu osobie wnioskującej.

9.1.5. IOD podejmuje decyzję o formie, w której zostanie przekazana kopia danych oraz wysokościach opłat za wszelkie kolejne kopie.

9.1.6. IOD ma prawo odmowy przekazania kopii danych osobowych w przypadku, gdy może to wpłynąć na prawa i wolności innych osób. Osoba wnioskująca jest każdorazowo informowana o odmowie realizacji prawa oraz przyczynie takiej odmowy.

9.2. Prawa do sprostowania, usunięcia, ograniczenia, przenoszenia danych osobowych oraz sprzeciwu wobec ich przetwarzania

9.2.1. **Prawo do sprostowania** - każda osoba, której dotyczą dane ma prawo do żądania niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Występująca osoba, której dane dotyczą ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

9.2.2. **Prawo do usunięcia danych** („Prawo do bycia zapomnianym") - każda osoba, której dane dotyczą, ma prawo żądania niezwłocznego usunięcia jej danych osobowych.

9.2.3. **Prawo do ograniczenia przetwarzania** - każda osoba, której dane dotyczą, ma prawo żądania od ADO ograniczania przetwarzania jej danych osobowych.

9.2.4. **Prawo do przenoszenia danych** - osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła ADO, oraz ma prawo przesłać te dane osobowe innemu administratorowi danych osobowych bez przeszkód ze strony ADO, któremu dostarczono te dane osobowe.

9.2.5. **Prawo do sprzeciwu** - osoba, której dane dotyczą ma prawo wnieść sprzeciw wobec przetwarzania jej danych osobowych.

9.3. Zasady realizacji praw osób, których dane dotyczą

9.3.1. Wnioski o realizację praw osób, których dane dotyczą kierowane są na adres do [iod@t4b.com.pl].

9.3.2. W przypadku, gdy wniosek zostanie skierowany do pracownika Spółki., należy przekazać go do IOD.

9.3.3. IOD dokonuje analizy wniosku oraz weryfikuje zasadność realizacji prawa osoby, której dane dotyczą.

9.3.4. W przypadku braku zasadności realizacji prawa, IOD zobligowany jest do niezwłocznego (nie dłuższego niż 1 miesiąc od daty wpływu wniosku do Spółki) przekazania tej informacji osobie wnioskującej wraz z właściwym uzasadnieniem decyzji.

9.3.5. W przypadku pozytywnej oceny wniosku, IOD zobligowany jest do wszczęcia postępowania mającego na celu realizację prawa osoby wnioskującej.

9.3.6. Realizacja prawa osoby, której dane dotyczą wymaga współpracy IOD z użytkownikami systemów informatycznych oraz AST oraz pracownikami przetwarzającymi dane osobowe w formie tradycyjnej (papierowej).

9.3.7. W celu realizacji prawa osoby, której dane dotyczą, IOD kontaktuje się z AST w celu wykonania czynności w systemie informatycznym wynikającym z prawa, które ma zostać zrealizowane.

9.3.8. AST, po wykonaniu czynności zleconych przez IOD przekazuje niezbędne materiały i/lub informacje o wykonaniu tych czynności do IOD.

9.3.9. Jeżeli czynności związane z realizacją prawa osoby, której dane dotyczą nie wymagają udziału użytkownika, IOD przekazuje informacje o konieczności wykonania czynności w systemach informatycznych do właściwych użytkowników systemów.

9.3.10. Użytkownicy po wykonaniu czynności zleconych przez IOD przekazuje niezbędne materiały i/lub informacje o realizacji prawa do IOD.

9.3.11. W sytuacji, w której realizacja prawa osoby, której dane dotyczą wymaga zaangażowania pracowników Spółki przetwarzających dane osobowe w wersji tradycyjnej (papierowej), na wniosek IOD pracownicy są zobligowani do wykonania zadań niezbędnych do realizacji prawa wnioskującego oraz przekazania informacji zwrotnej o wykonaniu zadań do IOD.

9.3.12. Po zakończeniu działań związanych z realizacją prawa osoby wnioskującej, IOD informuje o tym fakcie osobę wnioskującą. W przypadku, gdy czas realizacji prawa może przekroczyć 1 miesiąc od daty wpływu wniosku do Spółki, IOD przekazuje osobie wnioskującej odpowiedź wraz z planowanym terminem realizacji prawa, o które wnioskowała.

9.3.13. W przypadku realizacji prawa osoby, której dane dotyczą, IOD ma obowiązek przekazania informacji o konieczności realizacji tego prawa do wszystkich podmiotów, którym powierzono dane do przetwarzania oraz uzyskania informacji o jej realizacji.

10. Realizacja udostępnień danych osobowych

10.1. Dane osobowe udostępniane są wyłącznie na pisemny, umotywowany wniosek chyba, że przepisy prawa stanowią inaczej.

10.2. Udostępnienia danych osobowych może dokonać wyłącznie IOD.

10.3. Wszyscy pracownicy Spółki, w przypadku otrzymania wniosku o udostępnienie danych osobowych, zobligowani są do przekazania wniosku właściwemu IOD.

10.4. Wniosek powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie.

10.5. Zgodę na udostępnienie danych osobowych wydaje IOD w uzgodnieniu z pracownikami komórki organizacyjnej świadczącej wsparcie prawne, jeżeli uzna to za stosowne.

10.6. W przypadku wyrażenia zgody na udostępnienie, IOD przygotowuje udostępniane dane osobowe oraz odnotowuje fakt udostępnienia w Rejestrze udostępnień danych osobowych.

10.7. W przypadku udostępniania danych z systemów informatycznych, które nie odnotowują udostępnienia automatycznie, plik przekazywanych danych jest przechowywany przez IOD wraz z dokumentem wskazującym na podstawę udostępnienia i dodatkowym opisem wskazującym datę udostępnienia danych oraz określeniem odbiorcy danych (np. nazwa i adres instytucji).

10.8. Wzór rejestru udostępnień stanowi Załącznik nr 2 do niniejszych Zasad.

11. Zasady powierzenia danych osobowych

11.1. Zasady dotyczące powierzenia przetwarzania danych osobowych określone w niniejszym punkcie dotyczą sytuacji, w których Spółka korzysta z usług stron trzecich przekazując im dane osobowe, których jest administratorem.

11.2. Do powierzenia przetwarzania danych osobowych może dojść w każdej umowie bez względu na jej przedmiot.

11.3. Powierzenie przetwarzania danych osobowych przez spółkę z Grupy Przedsiębiorstw T4B podmiotom zewnętrznym następuje wyłącznie w drodze umowy powierzenia przetwarzania danych osobowych lub umowy wzajemnego powierzenia przetwarzania danych osobowych, zawartej na piśmie.

11.4. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych, nie może powierzyć do dalszego przetwarzania powierzonych mu danych bez wyraźnej zgody ADO.

11.5. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych, zobowiązany jest przetwarzać powierzone mu dane wyłącznie w celach, które zostały wskazane w zawartej z nim umowie.

11.6. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych, zobowiązany jest do spełnienia mających zastosowanie wymagań prawnych w obszarze danych osobowych.

11.7. Umowa, która zawiera zapisy o powierzeniu przetwarzania danych osobowych powinna w szczególności zawierać elementy dotyczące:

11.7.1. przedmiotu i czasu trwania przetwarzania danych osobowych,
11.7.2. charakteru i celu przetwarzania danych osobowych,
11.7.3. rodzaju danych osobowych oraz kategorii osób, których dane dotyczą,

11.7.4. obowiązków i praw ADO,
11.7.5. zobowiązań pracowników podmiotu przetwarzającego do zachowania powierzonych danych osobowych w poufności,
11.7.6. zapewnienia bezpieczeństwa organizacyjnego i technicznego przetwarzania danych osobowych,
11.7.7. zasad dalszego powierzania danych osobowych administrowanych przez spółkę z Grupy Przedsiębiorstw T4B,
11.7.8. udziału w procesie udzielania odpowiedzi na żądanie osoby, której dane dotyczą, oceny skutków dla przetwarzania danych osobowych, zgłaszania incydentów,
11.7.9. usunięciu lub zwróceniu powierzonych danych osobowych po zakończeniu świadczenia usługi,
11.7.10. udostępniania ADO wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w mających zastosowanie przepisach prawa w obszarze ochrony danych osobowych (np. audyty drugiej strony),
11.7.11. możliwości żądania natychmiastowego wstrzymania przetwarzania danych osobowych powierzonych w razie stwierdzenia niedostatecznej ochrony danych osobowych.

11.8. Dopuszcza się powierzenie przetwarzania danych osobowych z wykorzystaniem wzoru umowy dostarczonej przez podmiot zewnętrzny jedynie w sytuacji, w której w treści umowy znajdują się elementy wskazane w powyższym punkcie (10.7).

11.9. Wszyscy pracownicy Grupy Przedsiębiorstw T4B mają obowiązek zasięgnąć opinii IOD w każdej sytuacji, w której ma nastąpić podpisanie umowy, której przedmiot choćby pośrednio wiąże się z powierzeniem innej firmie danych osobowych bądź z przyjęciem przez Spółkę danych osobowych do przetwarzania.

11.10. W przypadku powierzenia przetwarzania danych osobowych zewnętrznym podmiotom świadczącym na rzecz spółek z Grupy Przedsiębiorstw T4B usługi o charakterze informatycznym (np. zewnętrzne serwery lub rozwiązania chmurowe), należy zapewnić, iż rozwiązania świadczone przez rzeczone podmioty są bezpieczne, poprzez realizację audytów bezpieczeństwa wobec outsourcowanych usług informatycznych oraz zapewniają możliwość automatycznego raportowania incydentów związanych z bezpieczeństwem danych osobowych.

11.11. Podmiot zewnętrzny, któremu powierzono przetwarzanie danych osobowych, zobowiązany jest do niezwłocznego poinformowania spółkę z Grupy Przedsiębiorstw T4B, która podpisała umowę powierzenia, o naruszeniach ochrony danych osobowych.

12. Upoważnienia do przetwarzania danych osobowych

12.1. Przed uzyskaniem dostępu do przetwarzania danych osobowych, każdy pracownik zostaje formalnie upoważniony przez ADO do ich przetwarzania w zakresie niezbędnym do wykonywania swoich obowiązków służbowych.

12.2. Warunkiem uzyskania upoważnienia do przetwarzania danych osobowych jest odbycie szkolenia wstępnego z zakresu ochrony danych osobowych.

12.3. W celu ograniczenia dostępu do przetwarzanych danych osobowych oraz upoważnieniu pracowników do przetwarzania adekwatnego zakresu danych osobowych wykorzystuje się procedury zarządzania dostępem do systemów teleinformatycznych oraz pomieszczeń Spółki.

12.4. Przetwarzanie danych osobowych w zakresie wykraczającym ponad nadane uprawnienia jest zabronione i traktowane jako naruszenie ochrony danych osobowych.

13. Naruszenia ochrony danych osobowych

13.1. Każdy z pracowników Grupy Przedsiębiorstw T4B w przypadku zidentyfikowania zdarzenia mogącego stanowić incydent bezpieczeństwa informacji (w tym naruszenie ochrony danych osobowych), jest zobowiązany niezwłocznie poinformować o tym fakcie IOD.

13.2. Zdarzenia, mogące stanowić incydent bezpieczeństwa to między innymi:

13.2.1. nieuprawnione ujawnienie informacji (w tym danych osobowych) osobom trzecim,

13.2.2. zagubienie lub znalezienie kluczy lub kart do systemu kontroli dostępu, awaria systemy kontroli dostępu, obecność osób nieuprawnionych na terenie Spółki,

13.2.3. zagubienie lub znalezienie nienadzorowanych nośników danych (dokumenty papierowe, nośniki CD/DVD, pendrive),

13.2.4. otrzymanie wiadomości e-mail posiadających znamiona ataku, zawierających zainfekowane załączniki, pochodzących z podejrzanych źródeł,

13.2.5. anomalie w funkcjonowaniu systemów informatycznych, pojawiające się powiadomienia z systemów antywirusowych,

13.2.6. utrata, zagubienie, kradzież urządzeń i nośników przetwarzających informacje.

13.3. W uzasadnionych przypadkach osoba, która zgłosiła zdarzenie zobowiązana jest postępować zgodnie z wytycznymi IOD lub wskazanej przez niego osoby odpowiedzialnej za obsługę zgłoszenia w zakresie zabezpieczenia materiału dowodowego. Jeśli zajdzie taka potrzeba, osoba zgłaszająca zdarzenie jest zobowiązana do zaprzestania wykonywania obowiązków służbowych w celu nienaruszania materiałów dowodowych.

13.4. IOD podejmuje decyzję, czy otrzymane zgłoszenie kwalifikuje się jako naruszenie ochrony danych osobowych.

13.5. W przypadku zakwalifikowania zdarzenia jako naruszenie ochrony danych osobowych, IOD po konsultacjach z ADO niezwłocznie zgłasza organowi nadzorczemu fakt wystąpienia zdarzenia mogącego naruszyć bezpieczeństwo danych osobowych.

13.6. Zgłoszenie naruszenia ochrony danych osobowych do organu nadzorczego musi nastąpić niezwłocznie, nie później niż w ciągu 72 godzin od jego stwierdzenia.

13.7. Jeżeli istnieje małe prawdopodobieństwo, iż naruszenie ochrony danych osobowych skutkować będzie naruszeniem praw lub wolności osób fizycznych, IOD nie jest zobligowany do zgłoszenia takiego naruszenia do organu nadzorczego.

13.8. Wszystkie zdarzenie zakwalifikowane jako naruszenie ochrony danych osobowych należy udokumentować w Rejestrze naruszeń ochrony danych osobowych zgodnie z wzorem stanowiącym Załącznik nr 3 do niniejszej Polityki.

13.9. W przypadku, gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób, których dotyczy naruszenie, należy je bez zbędnej zwłoki o tym poinformować o ile jest to technicznie możliwe.

13.10. W przypadku konieczności poinformowania osób, których dane dotyczą o naruszeniu ochrony danych osobowych, IOD wraz z ADO podejmują decyzję o kanale komunikacji oraz ustalają treść komunikatu.

14. Audyt ochrony danych osobowych

14.1. IOD jest zobowiązany do prowadzenia cyklicznych audytów przestrzegania zasad ochrony danych osobowych opisanych w regulacjach wewnętrznych Grupy Przedsiębiorstw T4B oraz mających zastosowanie wymaganiach prawnych. Zaleca się, aby audyty ochrony danych osobowych prowadzone były z co najmniej roczną częstotliwością.

14.2. Podczas określania zakresu audytu ochrony danych osobowych należy wziąć pod uwagę w szczególności:

14.2.1. obszary, w których zostały zidentyfikowane naruszenia ochrony danych osobowych,
14.2.2. rezultaty wcześniejszych audytów ochrony danych osobowych,
14.2.3. zmiany w otoczeniu wewnętrznym i zewnętrznym organizacji,
14.2.4. informację zwrotną od zainteresowanych stron.

14.3. Audytowi ochrony danych osobowych podlegają:

14.3.1. systemy informatyczne przetwarzające dane osobowe (zgodność funkcjonalności i zabezpieczeń systemów z mającymi zastosowanie regulacjami prawnymi),
14.3.2. zabezpieczenia fizyczne (zabezpieczenia pomieszczeń i budynków, w których przetwarzane są dane osobowe),
14.3.3. zabezpieczenia organizacyjne (m.in. procedury komunikacji i informowania o naruszeniach, powołanie ról i odpowiedzialności, aktualność wewnętrznych aktów normatywnych),
14.3.4. bezpieczeństwo osobowe (m.in. świadomość pracowników, realizacja szkoleń wstępnych i okresowych, aktualność uprawnień w systemach informatycznych) oraz
14.3.5. zgodność stanu faktycznego z wymaganiami mających zastosowanie aktów prawnych oraz wewnętrznych aktów normatywnych Grupy Przedsiębiorstw T4B

14.4. Do przeprowadzania audytu ochrony danych osobowych upoważniony jest IOD lub osoba przez niego wyznaczona posiadająca niezbędną wiedzę i kwalifikacje.

14.5. Po wykonanym audycie osoba przeprowadzająca audyt przygotowuje i przekazuje raport z audytu ADO.

14.6. W przypadku wystąpienia braku zgodności z wymaganiami prawnymi lub regulacjami wewnętrznymi, IOD inicjuje adekwatne działania mitygujące zidentyfikowane ryzyko lub ryzyka.

15. Szkolenia

15.1. Każdy pracownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub danymi osobowymi w wersji papierowej powinien być poddany przeszkoleniu w zakresie ochrony danych osobowych.

15.2. Za przeprowadzenie szkolenia odpowiada IOD.

15.3. Szkolenie powinno obejmować zaznajomienie pracownika z wymaganiami w zakresie ochrony danych osobowych zawartymi w mających zastosowanie przepisach prawa oraz regulacjach wewnętrznych obowiązujących w Grupie PrzedsiębiorstwT4B.

15.4. Każdorazowo w przypadku zmiany wymagań prawnych w zakresie ochrony danych osobowych, IOD jest zobowiązany do zapewnienia skutecznego przekazania tych zmian pracownikom Spółki.

15.5. IOD jest zobowiązany do budowania świadomości i organizacji cyklicznych szkoleń lub kampanii informacyjnych poświęconych tematyce ochrony danych osobowych oraz podstawowych zasad ochrony danych osobowych. Zaleca się, aby każdy pracownik Spółki, przetwarzający dane osobowe, brał obowiązkowo udział w takim szkoleniu nie rzadziej niż raz na 3 lata.

15.6. Opisywane powyżej szkolenia mogą odbywać się w dowolnej formie, ogólnie przyjętej u ADO.

16. Retencja danych

16.1. Dane osobowe przetwarzane w Grupie Przedsiębiorstw T4B przechowywane są przez okres nie dłuższy niż jest to niezbędne. Okres przechowywania danych jest dostosowywany do celu, w którym zostały zebrane.

16.2. Okres retencji może:

16.2.1. wynikać z powszechnie obowiązujących przepisów prawa lub regulacji wewnętrznych Spółki,

16.2.2. zostać określony przez organ nadzorczy w zakresie ochrony danych osobowych,

16.2.3. być ustalany przez komórki organizacyjne będące właścicielami przetwarzanych danych osobowych,

16.2.4. lub wynikać z zapisów konkretnej umowy.

16.3. Wskazany przez komórkę organizacyjną okres retencji jest weryfikowany i akceptowany przez IOD.

16.4. Okres retencji danych osobowych odnotowany jest w Rejestrze czynności przetwarzania w stosunku do określonej kategorii danych osobowych i celu, w jakim zostały one zebrane.

16.5. W przypadku dokumentacji w formie papierowej, za zniszczenie danych po ustaniu okresu retencji odpowiedzialny jest każdy pracownik przetwarzający te dane. Dane powinny zostać zniszczone w sposób uniemożliwiający ich odtworzenie. Proces

niszczenia nośników zawierających dane osobowe może zostać zlecony na zewnątrz organizacji.

16.6. W przypadku danych osobowych przetwarzanych w systemach informatycznych, każdy pracownik przetwarzający te dane jest odpowiedzialny, za usunięcie tych danych lub w przypadku braku technicznej możliwości usunięcia danych przez pracownika, zgłoszenie potrzeby ich usunięcia do IOD. Na podstawie tego wniosku, IOD kontaktuje się z AST w celu usunięcia danych przetwarzanych w wersji elektronicznej.

16.7. Co najmniej raz w roku kierownicy komórek organizacyjnych w spółkach Grupy Przedsiębiorstw T4B odpowiedzialni są za przeprowadzenie weryfikacji czy cel przetwarzania danych osobowych w stosunku do danych, które przetwarzają, jest nadal aktualny oraz czy nie przetwarzają danych dłużej aniżeli zostało to określone w Rejestrze czynności przetwarzania.

16.8. Wyniki przeglądu są przekazywane do IOD na jego wniosek.

17. Analiza ryzyka przetwarzania danych osobowych w Grupie Przedsiębiorstw T4B.

17.1. Ocena skutków dla ochrony danych osobowych jest procesem realizowanym w celu:

17.1.1. systematycznego opisu planowanych operacji przetwarzania i celów przetwarzania danych osobowych,

17.1.2. oceny czy operacje przetwarzania są niezbędne oraz proporcjonalne do celów,

17.1.3. oceny ryzyka naruszenia praw lub wolności osób, których dane dotyczą,

17.1.4. planowania zarządzania ryzykiem, w tym zabezpieczeń (organizacyjnych i technicznych) oraz środków i mechanizmów bezpieczeństwa mających zapewnić ochronę danych osobowych i wykazać przestrzeganie mających zastosowanie regulacji prawnych.

17.2. Proces oceny skutków dla ochrony danych osobowych jest realizowany cyklicznie i inicjowany przez IOD lub każdorazowo, gdy zajdzie taka potrzeba (np. wdrożenie nowego systemu informatycznego).

17.3. W proces oceny skutków dla ochrony danych zaangażowani są właściciele biznesowi oraz administratorzy zasobów.

17.4. Wyniki oceny skutków dla ochrony danych osobowych oraz propozycje działań mitygujących w planie postępowania z ryzkiem przedstawiane są ADO w celu ich akceptacji i uruchomienia ich realizacji.

17.5. Szczegółowy opis czynności został określony w dokumencie „Metodyka analizy ryzyka przetwarzania danych osobowych w Grupie Przedsiębiorstw T4B" stanowiącym Załącznik nr 4 do niniejszej Polityki.

18. Prywatność w fazie projektowania i ustawieniach domyślnych

18.1. W przypadku tworzenia nowych usług, planowania procesów, czy wdrażania systemów informatycznych, wszędzie tam, gdzie może dochodzić do przetwarzania

danych osobowych, wykorzystuje się zasady podejścia systemowego uwzględniające prywatność na etapie projektowania.

18.2. Każdorazowo, wskazane powyżej działania wymagają weryfikacji planowanych czynności przetwarzania danych osobowych i uwzględnienia zagadnień opisanych w rozdziale 17 – „Analiza ryzyka przetwarzania danych osobowych w Grupie Przedsiębiorstw T4B".

18.3. Pracownicy Grupy Przedsiębiorstw T4B odpowiedzialni za realizację działań związanych z rozwojem usług, planowaniem nowych procesów, czy wdrażaniem systemów informatycznych, są odpowiedzialni za poinformowanie IOD oraz uwzględnienie opinii IOD w realizowanych projektach.

18.4. IOD wraz z Działem DevOps opracowują zakres wymagań, które powinny zostać uwzględnione w realizowanym projekcie oraz zakres wymagań dotyczących funkcjonalności wdrażanych systemów informatycznym oraz tam, gdzie to niezbędne, umożliwiających realizację praw osób, których dane dotyczą.

19. Postanowienia końcowe.

W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy rozporządzenia ogólnego o ochronie danych osobowych i innych ustaw, w tym ustawy o ochronie danych osobowych.

20. Załączniki

I. **Załącznik nr 1** – Rejestr czynności przetwarzania

II. **Załącznik nr 2** - Rejestr udostępnień danych osobowych

III. **Załącznik nr 3** – Rejestr naruszeń ochrony danych osobowych

IV. **Załącznik nr 4** - Metodyka analizy ryzyka przetwarzania danych osobowych w Grupie T4B.

PREZES ZARZĄDU
T4B SP. Z O.O.
ROBERT SZCZEPANKOWSKI

Metodyka analizy ryzyka przetwarzania danych osobowych w Grupie T4B

Określenie krytyczności zasobów przetwarzających dane osobowe

1. Analiza ryzyka przetwarzania danych osobowych realizowana jest w stosunku do zasobów przetwarzających dane osobowe.
2. Zasoby, w których przetwarzane są dane osobowe to w szczególności:
   a. **systemy teleinformatyczne** (obejmujące systemy dedykowane do przetwarzania informacji oraz systemy wspomagające),
   b. **pomieszczenia biurowe wraz z wyposażeniem**, w których przetwarzane są dane osobowe,
   c. **pomieszczenia specjalne** stanowiące pomieszczenia o podwyższonym poziomie bezpieczeństwa wraz z ich wyposażeniem (np. serwerownia, pomieszczenia kadrowe).
3. Właściciel biznesowy systemu oraz właściciel biznesowy pomieszczenia określa poziom krytyczności zasobu mając na uwadze zakres danych, w który jest w nim przetwarzany oraz połączone z nim czynności przetwarzania wskazane w Rejestrze Czynności Przetwarzania.

Przeprowadzenie analizy ryzyka

1. Dla każdego zasobu, w których przetwarzane są dane osobowe, lokalny administrator systemu lub administrator pomieszczenia, w którym są przetwarzane dane osobowe korzystając z opracowanego katalogu ryzyk, określa prawdopodobieństwo materializacji poszczególnych ryzyk.
2. Podczas prowadzonej analizy ryzyka dla systemów teleinformatycznych przetwarzających dane osobowe weryfikuje się również spełnienie mających zastosowanie wymagań prawnych nakładanych na systemy teleinformatyczne (m.in. w zakresie anonimizacji danych, pseudonimizacji danych, możliwości realizacji praw osób, których dane dotyczą).

PRAWDOPODOBIEŃSTWO		OPIS
1	**Prawie niemożliwe**	Ryzyko raczej nie wystąpi lub możliwość jego wystąpienia jest znikoma (poniżej 30 %).
2	**Prawdopodobne**	Wystąpienie ryzyka jest realne (30% – 70%).
3	**Prawie pewne**	Istnieją racjonalne przesłanki by oceniać, że ryzyko zmaterializuje się w najbliższym czasie (powyżej 70%).

3. Do oceny prawdopodobieństwa materializacji ryzyka stosuje się poniższą skalę.

4. Na podstawie oceny krytyczności zasobów oraz prawdopodobieństwa utraty bezpieczeństwa danych osobowych określana jest wartość ryzyka zgodnie z poniższą macierzą.

5. Dla ryzyk:
   a. oszacowanych jako wysokie (określone kolorem czerwonym) konieczne jest dokładne opisanie problemu i propozycji działań, które zostaną wykorzystane do określenia Planu postępowania z ryzykiem.
   b. oszacowanych jako średnie (oznaczone kolorem żółtym) należy wskazać uzasadnienie poziomu ryzyka oraz rozważyć wskazanie działań do Planu postępowania z ryzykiem, jeśli jest to konieczne.
   c. oszacowanych jako niskie (określone kolorem zielonym) należy wskazać uzasadnienie poziomu ryzyka oraz je zaakceptować.
6. Dodatkowo, lokalny administrator systemu i administrator pomieszczenia opisują stosowane zabezpieczenia oraz określa ich skuteczność posługując się poniższą skalą:

SKUTECZNOŚĆ STOSOWANYCH ZABEZPIECZEŃ

3	Wysoka skuteczność stosowanych zabezpieczeń – brak elementów wymagających poprawy, mechanizm funkcjonuje bez zastrzeżeń.
2	Średnia skuteczność stosowanych zabezpieczeń - występują elementy wymagające nieznacznej poprawy, mechanizmy funkcjonują w sposób formalny, lecz pojawiają się nieznaczne uchybienia w jego stosowaniu.
1	Niska skuteczność zabezpieczeń – występują elementy wymagające znacznej poprawy.

7. Ocena ryzyka dokonywana jest z wykorzystaniem przygotowanych arkuszy analizy ryzyka lub dedykowanego narzędzia informatycznego. Arkusz analizy ryzyka obejmuje przynajmniej:
   - nazwę ocenianego zasobu,
   - poziom krytyczności zasobu,
   - imię i nazwisko lokalnego administratora systemu lub administratora pomieszczenia,
   - oceniane ryzyko,
   - opis zidentyfikowanych problemów/podatności,
   - poziom prawdopodobieństwa materializacji ryzyka,
   - wartość ryzyka (iloczyn poziomu krytyczności zasobu i prawdopodobieństwa materializacji ryzyka),
   - opis wykorzystywanych zabezpieczeń,
   - ocenę skuteczności wdrożonych zabezpieczeń,
   - decyzję o akceptacji ryzyka.
8. Dodatkowym dokumentem umożliwiającym przeprowadzenie analizy ryzyka jest katalog ryzyk obejmujący zestawienie możliwych zagrożeń właściwych dla poszczególnych kategorii zasobów tj. systemów teleinformatycznych i pomieszczeń.

Określenie Planu postępowania z ryzykiem

1. Dla zidentyfikowanych ryzyk nieakceptowalnych przygotowywane są Plany postępowania z ryzykiem opisywane w arkuszu analizy ryzyka.
2. W Planie Postępowania z Ryzykiem definiowane są następujące elementy:
   a. opis planowanych działań,
   b. ocenę poziomu ryzyka szczątkowego (po wdrożeniu mechanizmów wynikających z planu postępowania z ryzykiem),
   c. koszty wdrożeniowe i utrzymaniowe (jeżeli możliwe jest ich oszacowanie),
   d. osoba odpowiedzialna za realizację działania,
   e. termin realizacji.

T4B PREZES ZARZĄDU T4B SP. Z O.O. ROBERT SZCZEPANKOWSKI

Rejestr udostępnień danych osobowych							
Lp.	Podmiot, któremu udostępniono dane osobowe [nazwa i dane dane adresowe]	Data udostępnienia	Numer udostępnienia	Cel i podstawa prawna udostępnienia	Opis udostępnionych kategorii osób, których dane dotyczą	Imię i nazwisko osoby / nazwa podmiotu, których dane udostępniono	Zakres udostępnionych danych

numer naruszenia	data i godzina otrzymania zgłoszenia	data i godzina wystąpienia naruszenia	źródło zgłoszenia naruszenia	opis zaistniałego naruszenia	ocena konsekwencji naruszenia	charakter naruszenia ochrony danych osobowych	liczba wpisów danych osobowych, których dotyczy naruszenie	decyzja o konieczności zgłoszenia do organu nadzorczego	opis środków zastosowanych w celu zaradzeniu naruszenia	ocena środków zastosowanych w celu zaradzeniu naruszenia	działania prewencyjne
numer/rok	j.w.	j.w.	kto zgłosił naruszenie (pracownik,podmiot przetwarzający klient), w jakiej formie trafiło naruszenie	j.w.	do czego mogło doprowadzić naruszenie?	opis kategorii i liczby osób, których dotyczyć może naruszenie	liczba rekordów, której może dotyczyć naruszenie	TAK/NIE zgodnie z wymaganiami RODO - decyzję podejmuje Inspektor wraz z ADO	jakie środki zostały podjęte w celu niwelacji skutków wystąpienia naruszenia? Opis działań naprawczych	wypełniane na zakończeniu obsługi naruszenia. Ocena, czy środki były wystarczające	opis zabezpieczeń, które należy wdrożyć w przyszłości, aby nie doprowadzić do kolejnych naruszeń

Nazwa oraz dane kontaktowe Administratora Danych Osobowych Imię i nazwisko oraz dane kontaktowe IOD					Rejestr czynności przetwarzania												Zgody i obowiązki informacyjne	
lp.	Komórka organizacyjna	Opis kategorii osób, których dane dotyczą	Cel przetwarzania danych osobowych	Podstawa prawna przetwarzania	Źródło danych osobowych	Opis kategorii danych osobowych	Wrażliwe dane osobowe	Lokalizacja, w których przetwarzane są dane osobowe	Systemy informatyczne, w których przetwarzane są dane osobowe	Zbiory Papierowe	Planowany termin usunięcia danych osobowych	Zabezpieczenia organizacyjne i techniczne	Powierzanie danych osobowych	Dalsze powierzanie	Udostępnianie danych osobowych	Czy dane osobowe zostały przekazane do państwa	Zgoda	Obowiązek
1																		
2																		
3																		
4																		
5																		
6																		
7																		
8																		
9																		
10																		
11																		
12																		