POLITYKA OCHRONY DANYCH OSOBOWYCH W

Business Tours Maciej Tryba
ul. Borelowskiego 17B; 42-218 Częstochowa

pod marką Unique Poland.

O

Niniejszy dokument zatytułowany „**Polityka ochrony danych osobowych**” (dalej jako **Polityka**) ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w Business Tours Maciej Tryba, ul. Borelowskiego 17B; 42-218 Częstochowa (dalej jako **UNIQUE POLAND**).

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).

1. Polityka zawiera:
   a) opis zasad ochrony danych obowiązujących w UNIQUE POLAND;
   b) odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach);
2. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest właściciel UNIQUE POLAND .

UNIQUE POLAND powinna też zapewnić zgodność postępowania partnerów UNIQUE POLAND z niniejszą Polityką w odpowiednim zakresie, gdy dochodzi do przekazania im danych osobowych przez UNIQUE POLAND.

3. **Skróty i definicje:**
   a) **Polityka** oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.
   b) **RODO** oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).
   c) **Dane** oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.
   d) **Dane wrażliwe** oznaczają dane specjalne i dane karne.

e) **Dane specjalne (szczególnej kategorii)** oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

f) **Dane karne** oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.

g) **Dane dzieci** oznaczają dane osób poniżej 16. roku życia.

h) **Osoba** oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.

i) **Podmiot przetwarzający** oznacza organizację lub osobę, której UNIQUE POLAND powierzyła przetwarzanie danych osobowych (np. usługodawca IT, zewnętrzna księgowość).

j) **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.

k) **Eksport danych** oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.

l) **RCPD lub Rejestr** oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

m) **UNIQUE POLAND** oznacza - UNIQUE POLAND ul. Borelowskiego 17B; 42-218 Częstochowa

4. **Ochrona danych osobowych w UNIQUE POLAND – zasady ogólne**

5. **Filary ochrony danych osobowych w UNIQUE POLAND:**

   a) **Legalność** − UNIQUE POLAND dba o ochronę prywatności i przetwarza dane zgodnie z prawem.

   b) **Bezpieczeństwo** − UNIQUE POLAND zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.

c) **Prawa Jednostki** − UNIQUE POLAND umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.

d) **Rozliczalność** − UNIQUE POLAND dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

6. **Zasady ochrony danych**

UNIQUE POLAND przetwarza dane osobowe z poszanowaniem następujących zasad:

a) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);

b) rzetelnie i uczciwie (rzetelność);

c) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);

d) w konkretnych celach i nie „na zapas" (minimalizacja);

e) nie więcej niż potrzeba (adekwatność);

f) z dbałością o prawidłowość danych (prawidłowość);

g) nie dłużej niż potrzeba (czasowość);

h) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

7. **System ochrony danych**

System ochrony danych osobowych w UNIQUE POLAND składa się z następujących elementów:

1) **Inwentaryzacja danych.** UNIQUE POLAND dokonuje identyfikacji zasobów danych osobowych w UNIQUE POLAND, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:

a) przypadków przetwarzania danych specjalnych i danych „kryminalnych" (**dane wrażliwe**);

b) przypadków przetwarzania danych osób, których UNIQUE POLAND nie identyfikuje (**dane niezidentyfikowane**/UFO);

c) przypadków przetwarzania danych dzieci;

d) profilowania;

e) współadministrowania danymi.

2) **Rejestr.** UNIQUE POLAND opracowuje, prowadzi i utrzymuje Rejestr Czynności Danych Osobowych w UNIQUE POLAND (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych w UNIQUE POLAND.

3) **Podstawy prawne.** UNIQUE POLAND zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:

   a) utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,

   b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy UNIQUE POLAND przetwarza dane na podstawie prawnie uzasadnionego interesu UNIQUE POLAND.

4) **Obsługa praw jednostki.** UNIQUE POLAND spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

   a) **Obowiązki informacyjne.** UNIQUE POLAND przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.

   b) **Możliwość wykonania żądań.** UNIQUE POLAND weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.

   c) **Obsługa żądań.** UNIQUE POLAND zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane.

   d) **Zawiadamianie o naruszeniach.** UNIQUE POLAND stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

5) **Minimalizacja.** UNIQUE POLAND posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:

   a) zasady zarządzania **adekwatnością** danych;

   b) zasady reglamentacji i zarządzania **dostępem** do danych;

c) zasady zarządzania okresem **przechowywania** danych i weryfikacji dalszej przydatności;

6) **Bezpieczeństwo.** UNIQUE POLAND zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii, której wzór stanowi załącznik nr 1 do niniejszej polityki

b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;

c) dostosowuje środki ochrony danych do ustalonego ryzyka, m.in. poprzez

- prowadzenie ewidencji przydziału kluczy, której wzór stanowi załącznik nr 2 do niniejszej polityki

- prowadzenie Listy osób, które zapoznały się z „Polityką Ochrony Danych Osobowych", której wzór stanowi załącznik nr 3 do niniejszej polityki.

- prowadzenie „ewidencji budynków", której wzór stanowi załącznik nr 4 do niniejszej polityki.

d) posiada instrukcję zarządzania systemem informatycznym, której wzór stanowi załącznik nr 5 do niniejszej polityki.

e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych − zarządza incydentami (Rejestr naruszeń), której wzór stanowi załącznik nr 6 do niniejszej polityki.

7) **Przetwarzający.** UNIQUE POLAND posiada zasady doboru przetwarzających dane na rzecz UNIQUE POLAND, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia. Wzór umowy powierzenia stanowi załącznik nr 7 do niniejszej polityki.

8) **Eksport danych.** UNIQUE POLAND weryfikuje czy nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.

9) ***Privacy by design.*** UNIQUE POLAND zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w UNIQUE POLAND uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

8. **Inwentaryzacja**

1) **Dane wrażliwe**

UNIQUE POLAND identyfikuje przypadki, w których przetwarza lub może przetwarzać dane wrażliwe – dane szczególnej kategorii (dane specjalne i dane karne).

2) **Dane niezidentyfikowane**

UNIQUE POLAND identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane.

3) **Profilowanie**

UNIQUE POLAND identyfikuje przypadki, w których dokonuje profilowania przetwarzanych danych, a w sytuacji zidentyfikowania przypadków profilowania i zautomatyzowanego podejmowania decyzji, UNIQUE POLAND wprowadzi odpowiednie mechanizmy w tym zakresie.

4) **Współadministrowanie**

UNIQUE POLAND identyfikuje przypadki współadministrowania danymi.

9. **Rejestr Czynności Przetwarzania Danych**

1) RCPD stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

2) UNIQUE POLAND prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe. Wzór RCPD stanowi załącznik nr 8 do niniejszej polityki.

3) Rejestr jest jednym z podstawowych narzędzi umożliwiających UNIQUE POLAND rozliczanie większości obowiązków ochrony danych.

4) W Rejestrze, dla każdej czynności przetwarzania danych, którą UNIQUE POLAND uznała za odrębną dla potrzeb Rejestru, UNIQUE POLAND odnotowuje co najmniej:

   a) Czynności Przetwarzania

   b) Cel Przetwarzania

   c) Podstawę Przetwarzania

   d) Właściciela Procesu

   e) Kategorie Osób

   f) Kategorie Danych

   g) Szczególne Kategorie Danych

   h) Kategorie Odbiorców

   i) Sposób Przetwarzania Danych

   j) Sposób pozyskiwania Danych

   k) Okres Przechowywania Danych

   l) Ogólny opis środków bezpieczeństwa Danych

   m) Transfer do Państwa Trzeciego

   n) Kategorie Transferowanych Danych

   o) Odbiorcę Danych

   p) Państwo Trzecie / Organizację Międzynarodową

   q) Podstawę Prawną Transferu

   r) Dokumentację Dotyczącą Odpowiednich Zabezpieczeń

   s) Datę Ostatniej Aktualizacji

10. **Podstawy przetwarzania**

1) UNIQUE POLAND dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

2) Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel UNIQUE POLAND) UNIQUE POLAND dookreśla podstawę w czytelny sposób, gdy jest to potrzebne. Np. dla zgody wskazując na jej zakres, gdy podstawą jest prawo – wskazując na konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy – wskazując na kategorie zdarzeń, w których się zmaterializują, uzasadniony cel – wskazując na konkretny cel, np. marketing własny, dochodzenie roszczeń.

3) UNIQUE POLAND wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

11. **Sposób obsługi praw jednostki i obowiązków informacyjnych**

1) UNIQUE POLAND dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

2) UNIQUE POLAND ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej UNIQUE POLAND informacji o prawach osób, sposobie skorzystania z nich w UNIQUE POLAND, w tym wymaganiach dotyczących identyfikacji, metodach kontaktu ze UNIQUE POLAND w tym celu itp.

3) UNIQUE POLAND dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

4) UNIQUE POLAND wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

5) W celu realizacji praw jednostki UNIQUE POLAND zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez UNIQUE POLAND, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,

6) UNIQUE POLAND dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

12. **Obowiązki informacyjne**

1) UNIQUE POLAND określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych. Wzór klauzuli informacyjnej stanowi załącznik nr 9 do niniejszej polityki.
2) UNIQUE POLAND informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
3) UNIQUE POLAND informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
4) UNIQUE POLAND informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.
5) UNIQUE POLAND określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam gdzie to jest.
6) UNIQUE POLAND informuje osobę o planowanej zmianie celu przetwarzania danych.
7) UNIQUE POLAND informuje osobę przed uchyleniem ograniczenia przetwarzania.
8) UNIQUE POLAND informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
9) UNIQUE POLAND informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
10) UNIQUE POLAND bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

13. **Żądania osób**

1) **Prawa osób trzecich**. Realizując prawa osób, których dane dotyczą, UNIQUE POLAND wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste

itp.), UNIQUE POLAND może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

2) **Nieprzetwarzanie**. UNIQUE POLAND informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

3) **Odmowa**. UNIQUE POLAND informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

4) **Dostęp do danych**. Na żądanie osoby dotyczące dostępu do jej danych, UNIQUE POLAND informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących.

5) **Kopie danych**. Na żądanie UNIQUE POLAND wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. UNIQUE POLAND wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest w oparciu o oszacowany jednostkowy koszt obsługi żądania wydania kopii danych.

6) **Sprostowanie danych**. UNIQUE POLAND dokonuje sprostowania nieprawidłowych danych na żądanie osoby. UNIQUE POLAND ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych UNIQUE POLAND informuje osobę o odbiorcach danych, na żądanie tej osoby.

7) **Uzupełnienie danych**. UNIQUE POLAND uzupełnia i aktualizuje dane na żądanie osoby. UNIQUE POLAND ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. UNIQUE POLAND nie musi przetwarzać danych, które są UNIQUE POLAND zbędne). UNIQUE POLAND może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez UNIQUE POLAND procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

8) **Usunięcie danych.** Na żądanie osoby, UNIQUE POLAND usuwa dane, gdy:

    a) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,

b) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,

c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,

d) dane były przetwarzane niezgodnie z prawem,

e) konieczność usunięcia wynika z obowiązku prawnego,

f) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej).

g) UNIQUE POLAND określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.

h) Jeżeli dane podlegające usunięciu zostały upublicznione przez UNIQUE POLAND, UNIQUE POLAND podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich.

i) W przypadku usunięcia danych, UNIQUE POLAND informuje osobę o odbiorcach danych, na żądanie tej osoby.

9) **Ograniczenie przetwarzania.**

a) UNIQUE POLAND dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

- osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,

- przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,

- UNIQUE POLAND nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,

- osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie UNIQUE POLAND zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

b) W trakcie ograniczenia przetwarzania UNIQUE POLAND przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.

c) UNIQUE POLAND informuje osobę przed uchyleniem ograniczenia przetwarzania.

d) W przypadku ograniczenia przetwarzania danych UNIQUE POLAND informuje osobę o odbiorcach danych, na żądanie tej osoby.

10) **Przenoszenie danych.** Na żądanie osoby UNIQUE POLAND wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, **jeśli** jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona UNIQUE POLAND, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych UNIQUE POLAND.

11) **Sprzeciw w szczególnej sytuacji.** Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez UNIQUE POLAND w oparciu o uzasadniony interes UNIQUE POLAND lub o powierzone UNIQUE POLAND zadanie w interesie publicznym, UNIQUE POLAND **uwzględni** sprzeciw, o ile nie zachodzą po stronie UNIQUE POLAND ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

12) **Sprzeciw przy badaniach naukowych, historycznych lub celach statystycznych.** Jeżeli UNIQUE POLAND prowadzi badania naukowe, historyczne lub przetwarza dane w celach statystycznych, osoba może **wnieść** umotywowany jej szczególną sytuacją sprzeciw względem takiego przetwarzania. UNIQUE POLAND uwzględni taki sprzeciw, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

13) **Sprzeciw względem marketingu bezpośredniego.** Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez UNIQUE POLAND na potrzeby marketingu

bezpośredniego (w tym **ewentualnie** profilowania), UNIQUE POLAND uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

14) **Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu.** Jeżeli UNIQUE POLAND przetwarza dane w sposób automatyczny, w tym w szczególności profiluje osoby, i w konsekwencji podejmuje względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na osobę, UNIQUE POLAND zapewnia możliwość odwołania się do interwencji i decyzji człowieka po stronie UNIQUE POLAND, chyba że taka automatyczna decyzja:

a) jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a UNIQUE POLAND;

lub

b) jest wprost dozwolona przepisami prawa;

lub

c) opiera się o wyraźną zgodę odwołującej osoby.

14. MINIMALIZACJA

UNIQUE POLAND dba o minimalizację przetwarzania danych pod kątem:

a) adekwatności danych do celów (ilości danych i zakresu **przetwarzania**),
b) dostępu do danych,
c) czasu przechowywania danych.

1) Minimalizacja zakresu

a) UNIQUE POLAND zweryfikowała zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.

b) UNIQUE POLAND dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok.

c) UNIQUE POLAND przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (*privacy by design*).

2) Minimalizacja dostępu

a) UNIQUE POLAND stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).

b) UNIQUE POLAND stosuje kontrolę dostępu fizycznego.

c) UNIQUE POLAND dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających. Wzór upoważnień stanowi załącznik nr 10 do niniejszej polityki.

d) UNIQUE POLAND dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje nie rzadziej niż raz na rok.

3) Minimalizacja czasu

a) UNIQUE POLAND wdraża mechanizmy kontroli cyklu życia danych osobowych w UNIQUE POLAND, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze.

b) Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów produkcyjnych UNIQUE POLAND, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez UNIQUE POLAND. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

15. BEZPIECZEŃSTWO

UNIQUE POLAND zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez UNIQUE POLAND.

1) Analizy ryzyka i adekwatności środków bezpieczeństwa

a) UNIQUE POLAND przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

- UNIQUE POLAND zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania − wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
- UNIQUE POLAND kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
- UNIQUE POLAND przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. UNIQUE POLAND analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

b) UNIQUE POLAND ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym UNIQUE POLAND ustala przydatność i stosuje takie środki i podejście jak:

- pseudonimizacja,

- szyfrowanie danych osobowych,

- inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

- środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. Jednym z takich środków jest „Polityka czystego biurka, której wzór stanowi załącznik nr 11 do niniejszej polityki.

2) Oceny skutków dla ochrony danych

UNIQUE POLAND dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.
UNIQUE POLAND stosuje metodykę oceny skutków przyjętą w UNIQUE POLAND.

3) Środki bezpieczeństwa

UNIQUE POLAND stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych.

Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w UNIQUE POLAND i są bliżej opisane w procedurach przyjętych przez UNIQUE POLAND dla tych obszarów.

4) **Zgłaszanie naruszeń**

UNIQUE POLAND stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.

16. PRZETWARZAJĄCY

1) UNIQUE POLAND posiada zasady doboru i weryfikacji przetwarzających dane na rzecz UNIQUE POLAND opracowane w celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na UNIQUE POLAND.
2) UNIQUE POLAND przyjęła minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące Załącznik nr 7 do Polityki – „Wzór umowy powierzenia przetwarzania danych".
3) UNIQUE POLAND rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia danych osobowych.

17. EKSPORT DANYCH

UNIQUE POLAND rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy (EOG w 2017 r. = Unia Europejska, Islandia, Lichtenstein i Norwegia).

18. PROJEKTOWANIE PRYWATNOŚCI

UNIQUE POLAND zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania.

W tym celu zasady prowadzenia projektów i inwestycji przez UNIQUE POLAND odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na

prywatność i ochronę danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

19. POSTANOWIENIA KOŃCOWE

Polityka ochrony danych osobowych w UNIQUE POLAND Sp. z o.o. ul. Głowackiego 6 lok. 3, 30-085 Kraków wchodzi w życie z dniem 25.05.2018 r.

Załącznik nr 4

Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe w zbiorach danych

Obszar przetwarzania danych osobowych – administrator danych					
Id	**Nazwa obszaru**	**Adres**	**Kod pocztowy**	**Miejscowość**	**Uwagi**
1.	Siedziba Business Tours Maciej Tryba	Ul. Borelowskiego 17B	42-218	Częstochowa	-

Obszary przetwarzania danych osobowych – powierzenie przetwarzania danych osobowych					
Id	**Nazwa obszaru**	**Adres**	**Kod pocztowy**	**Miejscowość**	**Uwagi**
1.	**Wolin Michał Woliński**	**ul. Parkowa 4, Katowice**	**40-590**	**Katowice**	

Załącznik nr 5

Instrukcja zarządzania systemem informatycznym

I. Postanowienia ogólne

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej „Instrukcją", określa procedury dotyczące zasad bezpieczeństwa przetwarzania danych osobowych oraz zasady postępowania administratora danych osobowych, osób przez niego wyznaczonych i użytkowników przetwarzających dane osobowe w UNIQUE POLAND Sp. z o.o. ul. Borelowskiego 17B, 42-218 Częstochowa zwanej dalej „Administratorem".

W systemach informatycznych służących do przetwarzania danych osobowych stosuje się środki bezpieczeństwa na poziomie wysokim.

II. Nadawanie uprawnień do przetwarzania danych osobowych oraz ich rejestrowanie w systemie informatycznym

1. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych, każdy użytkownik powinien zostać zapoznany przez przełożonego lub osobę wyznaczoną przez wspólników do zapewnienia zgodności działalności UNIQUE POLAND z ochroną danych osobowych z przepisami dotyczącymi ochrony danych osobowych oraz obowiązującymi u Administratora wewnętrznymi regulacjami w tym zakresie.
2. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą zostać dopuszczone, z zastrzeżeniem ust. 3, wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych, wydane przez administratora danych osobowych.
3. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych, mogą zostać dopuszczone również osoby, którym udzielono upoważnień do przetwarzania danych osobowych na podstawie porozumień zawartych w sprawie powierzenia przetwarzania danych osobowych.
4. Wydanie upoważnienia oraz rejestracja użytkownika w systemie informatycznym przetwarzającym dane osobowe następuje na wniosek przełożonego użytkownika.
5. Procedury wydawania i odwoływania upoważnień dla użytkowników do przetwarzania danych osobowych realizowane są według następujących zasad:

1. przełożony użytkownika składa do administratora danych osobowych pisemny wniosek o wydanie upoważnienia, który zawiera:
    1. imię i nazwisko użytkownika,
    2. stanowisko zajmowane przez użytkownika,
    3. nazwę zbioru danych osobowych oraz nazwę systemu informatycznego, do którego użytkownik będzie miał dostęp,
    4. zakres upoważnienia do przetwarzania danych osobowych,
    5. datę, z jaką upoważnienie ma być wydane,
    6. okres ważności upoważnienia;
2. oryginał upoważnienia zostaje przekazany użytkownikowi za potwierdzeniem odbioru, kopia zostaje włączona do akt osobowych użytkownika oraz przekazana do wiadomości przełożonego;
3. wyrejestrowania użytkownika z systemu informatycznego dokonuje się na wniosek administratora danych osobowych lub przełożonego użytkownika.

6. Osobie niebędącej pracownikiem Administratora, administrator danych udziela upoważnienia na wniosek osoby przetwarzającej dane osobowe lub zapewniającej obsługę administracyjną podmiotu.
7. Użytkownik niebędący pracownikiem Administratora otrzymuje oryginał upoważnienia za potwierdzeniem odbioru, natomiast kopia upoważnienia przechowywana jest w siedzibie administratora.
8. Przyznanie uprawnień do przetwarzania danych osobowych w systemie informatycznym polega na wprowadzeniu do systemu identyfikatora oraz hasła dla każdego użytkownika.
9. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który po raz pierwszy korzysta z systemu informatycznego, odpowiada administrator danych lub przełożony użytkownika.
10. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielany innej osobie.
11. Przełożeni użytkowników zobowiązani są pisemnie informować administratora danych osobowych lub osobę wyznaczoną do zapewnienia zgodności działalności UNIQUE POLAND z ochroną danych osobowych o każdej zmianie dotyczącej użytkowników mającej wpływ na zakres posiadanych uprawnień do przetwarzania danych osobowych.

III. Stosowane metody i środki uwierzytelniania użytkownika oraz procedury związane **z ich zarządzaniem i użytkowaniem**

1. Użytkownik uzyskuje dostęp do danych osobowych przetwarzanych w systemie informatycznym wyłącznie po podaniu identyfikatora i hasła.
2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu swojego identyfikatora.
3. Identyfikator składa się minimalnie z 4 znaków, które nie są rozdzielone spacjami ani znakami interpunkcyjnymi. Identyfikator jest tworzony przy użyciu małych liter, z wyłączeniem polskich znaków.
4. Użytkownik, z chwilą przystąpienia do pracy w systemie informatycznym, otrzymuje hasło początkowe i jest zobowiązany zmienić je natychmiast po rozpoczęciu pracy, na sobie tylko znany ciąg znaków.
5. Hasło składa się co najmniej z 6 znaków.
6. Hasło powinno zawierać małe i wielkie litery oraz cyfry i znaki specjalne.
7. System informatyczny wyposażony jest w mechanizmy wymuszające zmianę hasła po upływie 30 dni od dnia ostatniej jego zmiany.
8. Hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych i należy je zachować w tajemnicy, również po upływie jego ważności.
9. Użytkownik nie może udostępniać osobom nieuprawnionym swojego identyfikatora oraz hasła. Po uwierzytelnieniu w systemie, użytkownik nie może udostępniać osobom nieuprawnionym swojego stanowiska pracy.
10. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest niezwłocznie je zmienić oraz powiadomić o tym fakcie administratora bezpieczeństwa informacji.

IV. **Rozpoczęcie, zawieszenie i zakończenie pracy** przez **użytkowników systemu**

1. Użytkownik, rozpoczynając pracę na komputerze, loguje się do systemu informatycznego.
2. Dostęp do danych osobowych możliwy jest jedynie po dokonaniu uwierzytelnienia użytkownika.

3. Maksymalna liczba prób wprowadzenia hasła przy logowaniu się do systemu informatycznego wynosi 3. Po przekroczeniu tej liczby prób logowania system blokuje dostęp do zbioru danych na poziomie danego użytkownika.
4. W przypadku braku aktywności użytkownika na komputerze przez czas dłuższy niż 10 minut następuje automatyczne włączenie wygaszacza ekranu.
5. Monitory stanowisk komputerowych, na których przetwarzane są dane osobowe, znajdujące się w pomieszczeniach, gdzie przebywają osoby, które nie posiadają upoważnień do przetwarzania danych osobowych, należy ustawić w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
6. Przebywanie osób nieuprawnionych w pomieszczeniach znajdujących się na obszarze, w którym są przetwarzane dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania.
7. Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać na czas nieobecności osób upoważnionych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
8. Przed opuszczeniem stanowiska pracy użytkownik obowiązany jest:
   1) wylogować się z systemu informatycznego albo
   2) wywołać blokowany hasłem wygaszacz ekranu.
9. Kończąc pracę użytkownik obowiązany jest:
   1) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
   2) zabezpieczyć stanowisko pracy.
10. Wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe, przechowuje się w szafach zamykanych na klucz.

V. Tworzenie kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu, poprzez tworzenie kopii zapasowych.
2. Za tworzenie kopii zapasowych zbiorów danych osobowych odpowiedzialny jest administrator danych lub inna osoba przez niego wyznaczona.

3. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu informatycznego. Za przeprowadzanie tej procedury odpowiedzialny jest administrator danych.
4. Kopie zapasowe przechowywane są w szafie zamykanej na klucz.

VI. Sposób, miejsce i okres przechowywania elektronicznych nośników danych zawierających dane osobowe oraz kopii zapasowych

1. Użytkownicy nie mogą wynosić z terenu Administratora nośników danych z zapisanymi danymi osobowymi, bez zgody administratora danych osobowych lub osoby wyznaczonej do zapewnienia zgodności działalności UNIQUE POLAND z ochroną danych osobowych.
2. Okresowe kopie zapasowe wykonywane są na, płytach CD, DVD, taśmach lub innych nośnikach danych. Kopie przechowuje się w innych pomieszczeniach niż te, w których przechowywane są zbiory danych wykorzystywane na bieżąco. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie.
3. Dostęp do nośników z kopiami zapasowymi danych osobowych ma wyłącznie osoba wyznaczona do zapewnienia zgodności działalności UNIQUE POLAND z ochroną danych osobowych albo Administrator Danych Osobowych.
4. Usunięcie danych z systemu powinno zostać zrealizowane przy pomocy oprogramowania przeznaczonego do bezpiecznego usuwania danych z nośnika danych.
5. Za zniszczenie kopii zapasowych sporządzanych indywidualnie przez użytkownika odpowiada użytkownik.
6. Dane osobowe w postaci elektronicznej należy usuwać z nośnika danych w sposób uniemożliwiający ich ponowne odtworzenie, nie później niż po upływie 5 dni po wykorzystaniu tych danych, chyba, że z odrębnych przepisów wynika obowiązek ich przechowywania.
7. Nośniki danych podlegają komisyjnemu zniszczeniu w przypadku wycofania z eksploatacji sprzętu komputerowego, na którym przetwarzane były dane osobowe oraz po przeniesieniu danych osobowych do zbiorów danych w systemie informatycznym z nośników, których ponowne wykorzystanie nie jest możliwe. Z przeprowadzonych czynności sporządza się protokół.
8. Przez zniszczenie nośników danych należy rozumieć ich trwałe i nieodwracalne zniszczenie fizyczne do stanu uniemożliwiającego ich rekonstrukcję i odzyskanie danych.

VII. Sposób zabezpieczenia systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. Za ochronę antywirusową systemu informatycznego odpowiada Administrator Danych osobowych.
2. System antywirusowy zainstalowany jest w każdym komputerze z dostępem do danych Osobowych.
3. Programy antywirusowe są uaktywnione przez cały czas pracy każdego komputera w systemie informatycznym.
4. Wszystkie pliki otrzymywane z zewnątrz, jak również wysyłane na zewnątrz, podlegają automatycznemu sprawdzeniu przez system antywirusowy pod kątem występowania wirusów, z zastosowaniem najnowszej dostępnej wersji programu antywirusowego.
5. W przypadku pojawienia się wirusa, użytkownik obowiązany jest zaprzestać wykonywania jakichkolwiek czynności w systemie i niezwłocznie powiadomić o tym fakcie administratora danych osobowych lub osobę wyznaczoną do zapewnienia zgodności działalności UNIQUE POLAND z ochroną danych osobowych.
6. Niedozwolone jest wyłączanie, blokowanie i odinstalowywanie programów zabezpieczających komputer przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem (skaner antywirusowy, firewall).
7. Wszystkie pliki zawierające dane osobowe, wysyłane na zewnątrz jak również wewnątrz, podlegają konieczności zabezpieczenia/szyfrowania przy użyciu hasła (np. przy wykorzystaniu oprogramowania 7zip lub innego odpowiedniego).
   1) Hasło składa się co najmniej z 6 znaków i powinno zawierać małe i wielkie litery oraz cyfry i znaki specjalne.
   2) Odbiorca danych osobowych uzyskuje hasło dostępu do zabezpieczonych/szyfrowanych plików innym kanałem komunikacji, aniżeli drogą którą uzyskał zabezpieczone/zaszyfrowane pliki (np. telefonicznie, sms-em itp.)

VIII. Udostępnianie danych osobowych i sposób odnotowywania informacji o udostępnianiu danych

1. Dane osobowe przetwarzane u Administratora mogą być udostępnione osobom lub podmiotom uprawnionym do ich otrzymania, na mocy przepisów o ochronie danych osobowych oraz innych przepisów powszechnie obowiązujących.
2. Dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba, że przepisy odrębne stanowią inaczej.
3. Dane udostępnione Administratorowi przez inny podmiot można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

IX. Postępowanie w przypadku naruszenia ochrony danych osobowych

1. Każdy użytkownik, który stwierdza lub podejrzewa naruszenie ochrony danych w systemie informatycznym, zobowiązany jest niezwłocznie poinformować o tym administratora danych osobowych oraz osobę wyznaczoną do zapewnienia zgodności działalności UNIQUE POLAND z ochroną danych osobowych.
2. Do czasu przybycia na miejsce administratora danych osobowych lub osoby wyznaczonej do zapewnienia zgodności działalności UNIQUE POLAND z ochroną danych osobowych należy:
   1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców naruszenia;
   2) rozważyć wstrzymanie bieżącej pracy na komputerze w celu zabezpieczenia miejsca zdarzenia;
   3) zaniechać, o ile to możliwe, dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę;
   4) udokumentować wstępnie zaistniałe naruszenie;
   5) nie opuszczać, bez uzasadnionej potrzeby, miejsca zdarzenia do czasu przybycia administratora sieci lub administratora bezpieczeństwa informacji.
3. Po przybyciu na miejsce administrator danych osobowych lub osoba wyznaczona do zapewnienia zgodności działalności UNIQUE POLAND z ochroną danych osobowych:
   1) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania;

2) może żądać wyjaśnień dotyczących zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
3) dokonuje zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się skutków naruszenia;
4) podejmuje odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia;

4. Administrator danych osobowych dokumentuje zaistniały przypadek naruszenia oraz wypełnia rejestr naruszeń.

Załącznik nr 6

Rejestr naruszeń

Załącznik nr 7

Umowa

powierzenia przetwarzania danych osobowych

do Umowy .....

zawarta pomiędzy

Business Tours Maciej Tryba
Ul. Borelowskiego 17B; 42-218 Częstochowa

Jako Administratorem

a

..... jako Przetwarzającym

SPIS TREŚCI

Umowa

powierzenia przetwarzania danych osobowych

stanowiąca uzupełnienie Umowy .....

zawarta w dniu ..... w ....., pomiędzy:

Business Tours Maciej Tryba
Ul. Borelowskiego 17B; 42-218 Częstochowa
(„**Administrator**")

a

..... („**Przetwarzający**")

(dalej łącznie jako: „**Strony**")

Mając na uwadze, że:

Strony zawarły umowę ..... („Umowa Podstawowa"), w związku, z wykonywaniem której Administrator powierzy Przetwarzającemu przetwarzanie danych osobowych w zakresie określonym Umową;

Celem Umowy jest ustalenie warunków, na jakich Przetwarzający wykonuje operacje przetwarzania Danych Osobowych w imieniu Administratora;

Strony zawierając Umowę dążą do takiego uregulowania zasad przetwarzania Danych Osobowych, aby odpowiadały one w pełni postanowieniom rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej RODO.

Strony postanowiły zawrzeć Umowę o następującej treści:

- przedmiot i czas trwania przetwarzania,

- charakter i cel przetwarzania,

- rodzaj danych osobowych oraz kategorie osób, których dane dotyczą,

- obowiązki i prawa administratora

1. **Opis Przetwarzania**

1.1. Przedmiot [art. 28 ust. 3 RODO] Na warunkach określonych niniejszą Umową oraz Umową Podstawową Administrator powierza Przetwarzającemu przetwarzanie (w rozumieniu RODO) dalej opisanych Danych Osobowych.

1.2. Czas [art. 28 ust. 3 RODO] Przetwarzanie będzie wykonywane w okresie obowiązywania Umowy Podstawowej.

1.3. Charakter i cel [art. 28 ust. 3 RODO] Charakter i cel przetwarzania wynikają z Umowy Podstawowej. W szczególności:

1.3.1. charakter przetwarzania określony jest następującą rolą Przetwarzającego ……., zaś

1.3.2. celem przetwarzania jest ……..

1.4. Rodzaj danych [art. 28 ust. 3 RODO] Przetwarzanie obejmować będzie następujące rodzaje danych osobowych („Dane”):

Dane zwykłe

a) .....

Dane szczególnych kategorii i dane karne:

b) …….

Dane dzieci

c) .....

1.5. Kategorie osób [art. 28 ust. 3 RODO] Przetwarzanie Danych będzie dotyczyć następujących kategorii osób:

(1) .....,

(2) .....,

(3) .....,

2. **Podpowierzenie**

2.1. Podpowierzenie [art. 28 ust. 2 RODO] Przetwarzający może powierzyć konkretne operacje przetwarzania Danych („podpowierzenie”) w drodze pisemnej umowy podpowierzenia („Umowa Podpowierzenia”) innym podmiotom przetwarzającym.

(„Podprzetwarzający”), pod warunkiem uprzedniej akceptacji Podprzetwarzającego przez Administratora lub braku sprzeciwu.

2.2. Sprzeciw. Powierzenie przetwarzania Danych Podprzetwarzającym spoza Listy Zaakceptowanych Podprzetwarzających wymaga uprzedniego zgłoszenia Administratorowi w celu umożliwienia wyrażenia sprzeciwu. Administrator może z uzasadnionych przyczyn zgłosić udokumentowany sprzeciw względem powierzenia Danych konkretnemu Podprzetwarzającemu. W razie zgłoszenia sprzeciwu Przetwarzający nie ma prawa powierzyć Danych Podprzetwarzającemu objętemu sprzeciwem, a jeżeli sprzeciw dotyczy aktualnego Podprzetwarzającego, musi niezwłocznie zakończyć podpowierzenie temu Podprzetwarzającemu. Wątpliwości co do zasadności sprzeciwu i ewentualnych negatywnych konsekwencji Przetwarzający zgłosi Administratorowi w czasie umożliwiającym zapewnienie ciągłości przetwarzania.

2.3. Transfer obowiązków [art. 28 ust. 4 RODO] Dokonując podpowierzenia Przetwarzający ma obowiązek zobowiązać Podprzetwarzającego do realizacji wszystkich obowiązków Przetwarzającego wynikających z niniejszej Umowy powierzenia, z wyjątkiem tych, które nie mają zastosowania ze względu na naturę konkretnego podpowierzenia.

2.4. Zobowiązanie względem Administratora. Przetwarzający ma obowiązek zapewnić, aby Podprzetwarzający złożył Administratorowi zobowiązanie do wykonania obowiązków, o których mowa w poprzednim ustępie. Może to zostać wykonane przez podpisanie stosownego oświadczenia adresowanego do Administratora wraz z podpisaniem Umowy Podpowierzenia, zawierającego listę obowiązków Podprzetwarzającego.

2.5. Zakaz podzlecenia świadczenia głównego [art. 28 ust. 4 RODO] Przetwarzający nie ma prawa przekazać Podprzetwarzającemu całości wykonania Umowy.

3. Obowiązki Przetwarzającego

Przetwarzający ma następujące obowiązki:

3.1. Udokumentowane polecenia [art. 28 ust. 3 lit. a RODO] Przetwarzający przetwarza Dane wyłącznie zgodnie z udokumentowanymi poleceniami lub instrukcjami Administratora.

3.2. Nieprzetwarzanie poza EOG [art. 28 ust. 3 lit. a RODO] Przetwarzający oświadcza, że nie przekazuje Danych do państwa trzeciego lub organizacji międzynarodowej (czyli poza Europejski Obszar Gospodarczy („EOG")). Przetwarzający oświadcza również, że nie korzysta z podwykonawców, którzy przekazują Dane poza EOG.

3.3. Poinformowanie o zamiarze przetwarzania poza EOG. [art. 28 ust. 3 lit. a RODO] Jeżeli Przetwarzający ma zamiar lub obowiązek przekazywać Dane poza EOG, informuje o tym Administratora, w celu umożliwienia Administratorowi podjęcia decyzji i działań niezbędnych do zapewnienia zgodności przetwarzania z prawem lub zakończenia powierzenia przetwarzania.

3.4. Tajemnica [art. 28 ust. 3 lit. b RODO] Przetwarzający uzyskuje od osób, które zostały upoważnione do przetwarzania Danych w wykonaniu Umowy, udokumentowane zobowiązania do zachowania tajemnicy, ewentualnie upewnia się, że te osoby podlegają ustawowemu obowiązkowi zachowania tajemnicy.

3.5. Bezpieczeństwo [art. 28 ust. 3 lit. c RODO] Przetwarzający zapewnia ochronę Danych i podejmuje środki ochrony danych, o których mowa w art. 32 RODO, zgodnie z dalszymi postanowieniami Umowy.

3.6. Podprzetwarzanie [art. 28 ust. 3 lit. d RODO] Przetwarzający przestrzega warunków korzystania z usług innego podmiotu przetwarzającego (Podprzetwarzającego).

3.7. Współpraca przy realizacji praw jednostki [art. 28 ust. 3 lit. e RODO] Przetwarzający zobowiązuje się wobec Administratora do odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania praw określonych w rozdziale III RODO („Prawa jednostki"). Przetwarzający oświadcza, że zapewnia obsługę Praw jednostki w odniesieniu do powierzonych Danych. Szczegóły obsługi Praw jednostki zostaną pomiędzy Stronami uzgodnione. Strony ustaliły procedurę obsługi Praw jednostki odrębnym dokumentem.

3.8. Wsparcie przy obowiązkach bezpieczeństwa [art. 28 ust. 3 lit. f RODO] Przetwarzający współpracuje z Administratorem przy wykonywaniu przez Administratora

obowiązków z obszaru ochrony danych osobowych, o których mowa w art. 32−36 RODO (ochrona danych, zgłaszanie naruszeń organowi nadzorczemu, zawiadamianie osób dotkniętych naruszeniem ochrony danych, ocena skutków dla ochrony danych i uprzednie konsultacje z organem nadzorczym).

3.9. Legalność poleceń [art. 28 ust. 3 ak. 2 RODO] Jeżeli Przetwarzający powezmie wątpliwości co do zgodności z prawem wydanych przez Administratora poleceń lub instrukcji, Przetwarzający natychmiast informuje Administratora o stwierdzonej wątpliwości (w sposób udokumentowany i z uzasadnieniem), pod rygorem utraty możliwości dochodzenia roszczeń przeciwko Administratorowi z tego tytułu.

3.10. Projektowanie prywatności [art. 25 ust. 1 RODO] Planując dokonanie zmian w sposobie przetwarzania Danych, Przetwarzający ma obowiązek zastosować się do wymogu projektowania prywatności, o którym mowa w art. 25 ust. 1 RODO i ma obowiązek z wyprzedzeniem informować Administratora o planowanych zmianach w taki sposób i terminach, aby zapewnić Administratorowi realną możliwość reagowania, jeżeli planowane przez Przetwarzającego zmiany w opinii Administratora grożą uzgodnionemu poziomowi bezpieczeństwa Danych lub zwiększają ryzyko naruszenia praw lub wolności osób, wskutek przetwarzania Danych przez Przetwarzającego.

3.11. Minimalizacja [art. 25 ust. 2 RODO] Przetwarzający zobowiązuje się do ograniczenia dostępu do Danych Osobowych wyłącznie do osób, których dostęp do Danych jest potrzebny dla realizacji Umowy i posiadających odpowiednie upoważnienie.

3.12. RCPD [art. 30 ust. 2 RODO] Przetwarzający zobowiązuje się do prowadzenia dokumentacji opisującej sposób przetwarzania Danych, w tym rejestru czynności przetwarzania danych osobowych (wymóg art. 30 RODO), chyba że jest wyłączony z konieczności stosowania w/w rejestru na mocy art. 30 ust.5 RODO. Przetwarzający udostępniania na żądanie Administratora prowadzony rejestr czynności przetwarzania danych przetwarzającego, z wyłączeniem informacji stanowiących tajemnicę handlową innych klientów Przetwarzającego.

3.13. Profilowanie [art. 13 i 14 RODO] Jeżeli Przetwarzający wykorzystuje w celu realizacji Umowy zautomatyzowane przetwarzanie, w tym profilowanie, o którym

mowa w art. 22 ust. 1 i 4 RODO, Przetwarzający informuje o tym Administratora w celu i w zakresie niezbędnym do wykonania przez Administratora obowiązku informacyjnego.

3.14. Szkolenie personelu Przetwarzający ma obowiązek zapewnić osobom upoważnionym do przetwarzania Danych odpowiednie szkolenie z zakresu ochrony danych osobowych.

4. Obowiązki Administratora

4.1. Administrator zobowiązany jest współdziałać z Przetwarzającym w wykonaniu Umowy, udzielać Przetwarzającemu wyjaśnień w razie wątpliwości co do legalności poleceń Administratora, jak też wywiązywać się terminowo ze swoich szczegółowych obowiązków.

5. **Bezpieczeństwo danych**

5.1. Bezpieczeństwo danych osobowych [art. 32 RODO] Przetwarzający przeprowadził analizę ryzyka przetwarzania powierzonych Danych i stosuje się do jej wyników, co do organizacyjnych i technicznych środków ochrony danych.

5.2. Gwarancje bezpieczeństwa. Przetwarzający przedstawił Administratorowi informacje i dokumenty potwierdzające, że Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych. Obie Strony zachowują kopie przedstawionych dokumentów i dowody przedstawienia informacji, dla potrzeb spełnienia wymogu rozliczalności.

6. Powiadomienie o Naruszeniach Danych **Osobowych**

6.1. Powiadomienie o naruszeniu. Przetwarzający powiadamia Administratora danych o każdym podejrzeniu naruszenia ochrony Danych osobowych nie później niż w 24 godziny od pierwszego zgłoszenia, umożliwia Administratorowi uczestnictwo w czynnościach wyjaśniających i informuje Administratora o ustaleniach z chwilą ich dokonania, w szczególności o stwierdzeniu naruszenia.

6.2. Rozwinięcie. Powiadomienie o stwierdzeniu naruszenia, powinno być przesłane wraz z wszelką niezbędną dokumentacją dotyczącą naruszenia, aby umożliwić Administratorowi spełnienie obowiązku powiadomienia organ nadzoru.

7. **Nadzór**

7.1. Sprawowanie kontroli [art. 28 ust. 3 lit. h RODO] Administrator kontroluje sposób przetwarzania powierzonych Danych Osobowych po uprzednim poinformowaniu Przetwarzającego o planowanej kontroli. Administrator lub wyznaczone przez niego osoby są uprawnione do:

a) wstępu do pomieszczeń, w których przetwarzane są Dane Osobowe oraz

b) wglądu do dokumentacji związanej z przetwarzaniem Danych Osobowych.

c) Administrator uprawniony jest do żądania od Przetwarzającego udzielania informacji dotyczących przebiegu przetwarzania Danych Osobowych, oraz udostępnienia rejestrów przetwarzania.

7.2. Współpraca przy kontroli. [art. 28 ust. 3 lit. h RODO] Przetwarzający współpracuje z urzędem ochrony danych osobowych w zakresie wykonywanych przez niego zadań.

7.3. Przetwarzający:

a) udostępnia Administratorowi wszelkie informacje niezbędne do wykazania zgodności działania Administratora z przepisami RODO,

b) umożliwia Administratorowi lub upoważnionemu audytorowi przeprowadzanie audytów lub inspekcji. Przetwarzający współpracuje w zakresie realizacji audytów lub inspekcji.

8. **Oświadczenia** Stron

8.1. Oświadczenie Administratora. Administrator oświadcza, że jest Administratorem Danych oraz, że jest uprawniony do ich przetwarzania w zakresie, w jakim powierzył je Przetwarzającemu.

8.2. Oświadczenie Przetwarzającego [art. 28 ust. 1 RODO]. Przetwarzający oświadcza, że w ramach prowadzonej działalności gospodarczej profesjonalnie zajmuje się przetwarzaniem danych osobowych objętym Umowa i Umową Podstawową, posiada w tym zakresie niezbędną wiedzę, odpowiednie środki techniczne i organizacyjne oraz daje rękojmię należytego wykonania niniejszej Umowy.

8.3. Referencje [art. 28 ust. 1 RODO]. Na żądanie Administratora Przetwarzający okaże Administratorowi stosowne referencje, wykaz doświadczenia, informacje finansowe

lub inne dowody, iż Przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

9. **Odpowiedzialność**

9.1. Odpowiedzialność Przetwarzającego [art. 82 ust. 3 RODO] Przetwarzający odpowiada za szkody spowodowane swoim działaniem w związku z niedopełnieniem obowiązków, które RODO nakłada bezpośrednio na Przetwarzającego lub gdy działał poza zgodnymi z prawem instrukcjami Administratora lub wbrew tym instrukcjom. Przetwarzający odpowiada za szkody spowodowane zastosowaniem lub nie zastosowaniem właściwych środków bezpieczeństwa.

9.2. Odpowiedzialność za Podprzetwarzających [art. 28 ust. 4 RODO] Jeżeli Podprzetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków przez Podprzetwarzającego spoczywa na Przetwarzającym.

10. Okres Obowiązywania Umowy **Powierzenia** [art. 28 ust. 3 RODO]

10.1. Umowa została zawarta na czas obowiązywania Umowy Podstawowej.

11. **Usunięcie Danych**

11.1. Usunięcie danych [art. 28 ust. 3 lit g RODO] Z chwilą rozwiązania Umowy Przetwarzający nie ma prawa do dalszego przetwarzania powierzonych Danych i jest zobowiązany do:

a) usunięcia Danych,

b) usunięcia wszelkich ich istniejących kopii lub zwrotu Danych, chyba że Administrator postanowi inaczej lub prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują dalej przechowywanie Danych.

c) Strony uzgodnią sposób usunięcia Danych odrębnym dokumentem w ciągu 30 dni od zawarcia Umowy Powierzenia.

11.2. Karencja. Przetwarzający dokona usunięcia Danych po upływie 180 dni od zakończenia Umowy, chyba że Administrator poleci mu to uczynić wcześniej.

11.3. Oświadczenie. Po wykonaniu zobowiązania, o którym mowa w pkt 10.1., Przetwarzający złoży Administratorowi pisemne oświadczenie potwierdzające trwałe usunięcie wszystkich Danych.

12. **Postanowienia Końcowe**

12.1. Pierwszeństwo. W razie sprzeczności pomiędzy postanowieniami niniejszej Umowy Powierzenia a Umowy Podstawowej, pierwszeństwo mają postanowienia Umowy Powierzenia. Oznacza to także, że kwestie dotyczące przetwarzania danych osobowych pomiędzy Administratorem a Przetwarzającym należy regulować poprzez zmiany niniejszej Umowy lub w wykonaniu jej postanowień.

12.2. Egzemplarze. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

12.3. Właściwość prawa. Umowa podlega prawu polskiemu oraz RODO.

Załącznik nr 8

Rejestr czynności przetwarzania danych osobowych

Załącznik nr 9

Wzór klauzuli informacyjnej

Klauzula informacyjna ……..

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej **RODO** informuję, iż:

1. Administratorem Pani/Pana danych osobowych jest Business Tours Maciej Tryba, ul. Borelowskiego 17B; 42-218 Częstochowa;
2. Osobą wyznaczoną do zapewnienia zgodności działalności UNIQUE POLAND z ochroną danych osobowych jest Pan/Pani (*imię i nazwisko) Maciej Tryba (*e-mail służbowy lub nr tel. służbowego) biuro@btours.com.pl;
3. Pani/Pana dane osobowe przetwarzane będą w celu związanym z …….., na podstawie Pani/Pana dobrowolnej zgody, na podstawie art. 6 ust. 1 lit. a RODO;
4. odbiorcą Pani/Pana danych osobowych jest …….
5. Pani/Pana dane osobowe będą przechowywane przez okres ……;
6. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody na ich przetwarzanie w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody wyrażonej przed jej cofnięciem;
7. Ma Pan/Pani prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
8. Podanie przez Pana/Panią danych osobowych jest dobrowolne, ale konieczne dla celów związanych z nawiązaniem i przebiegiem Pani/Pana zatrudnienia;

/……./

Czytelny podpis

Załącznik nr 10

Wzór upoważnienia do przetwarzania danych osobowych

UPOWAŻNIENIE

DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej **RODO** – nadaję upoważnienie Pani/Panu:

……

(imię i nazwisko)

……

(stanowisko)

do przetwarzania danych osobowych w zakresie ……..tj. uzyskuje Pani/Pan upoważnienie do przetwarzania danych osobowych …….

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, Kodeksu pracy, a także z Polityką ochrony danych osobowych Pracodawcy.

Jednocześnie upoważniam Panią/Pana do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień, ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w
Business Tours Maciej Tryba
Ul. Borelowskiego 17B; 42-218 Częstochowa
.

Okres ważności

od: ……..

do: …….

……

podpis osoby uprawnionej do nadania upoważnienia

Data wygaśnięcia* ……..……..

Odwołano, dnia …….

……

podpis osoby uprawnionej do odwołania upoważnienia

* Data rozwiązania stosunku pracy/umowy cywilnoprawnej

Załącznik nr 11

Polityka czystego biurka

POLITYKA CZYSTEGO BIURKA

w

Business Tours Maciej Tryba
Ul. Borelowskiego 17B; 42-218 Częstochowa

Niniejsza polityka czystego biurka obowiązuje wszystkich pracowników zatrudnionych w **Business Tours Maciej Tryba, Ul. Borelowskiego 17B; 42-218 Częstochowa**

1. Za pracownika uważa się każdą osobę zatrudnioną na podstawie umowy o pracę, powołania, wyboru, mianowania lub spółdzielczej umowy o pracę, a także osobę fizyczną wykonującą pracę na innej podstawie niż stosunek pracy, doktoranta, studenta i ucznia, niebędący pracownikami, oraz wolontariusza, jak również osobę prowadzącą jednoosobową działalność gospodarczą, współpracującą z pracodawcą.
2. Za pracodawcę uważa się **Business Tours Maciej Tryba, Ul. Borelowskiego 17B; 42-218 Częstochowa**.
3. Każdy pracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są pracownikowi niezbędne w danym momencie pracy do wykonania bieżących zadań.
4. Po zakończonej pracy pracownik zobowiązany jest odłożyć wszystkie dokumenty zawierające dane osobowe do zamykanej na klucz szafy.

5. Po zakończonej pracy pracownik zobowiązany jest odłożyć laptopa do zamykanej na klucz szafy.
6. Po zakończonej pracy na biurku mogą znajdować się jedynie telefon i przybory biurowe, takie jak: zszywacz, dziurkacz, długopis, itp.
7. Pracownik zobowiązany jest do niszczenia dokumentów niepotrzebnych w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji, np. w niszczarce.
8. Niniejsza Polityka obowiązuje od dnia 25.05.2018 r.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych

osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej **RODO** – nadaję upoważnienie Pani/Panu:

……..

(imię i nazwisko)

…….

(stanowisko)

do przetwarzania danych osobowych w zakresie ……..

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, Kodeksu pracy, a także z Polityką ochrony danych osobowych Pracodawcy.

Jednocześnie upoważniam Panią/Pana do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień, ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w Business Tours Maciej Tryba, ul. Borelowskiego 17B;42-218 Częstochowa.

Okres ważności

od: ……..

do: *

……

podpis osoby uprawnionej do nadania upoważnienia

Data wygaśnięcia*

Odwołano, dnia …….

……

podpis osoby uprawnionej do odwołania upoważnienia

* Data rozwiązania stosunku pracy/umowy cywilnoprawnej

UPPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy

95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej **RODO** – nadaję upoważnienie Pani/Panu:

…….

(imię i nazwisko)

…….

(stanowisko)

do przetwarzania danych osobowych w zakresie ……...

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, Kodeksu pracy, a także z Polityką ochrony danych osobowych Pracodawcy.

Jednocześnie upoważniam Panią/Pana do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień, ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w Business Tours Maciej Tryba, ul. Borelowskiego 17B;42-218 Częstochowa.

Okres ważności

od: ……..

do: *

……

podpis osoby uprawnionej do nadania upoważnienia

Data wygaśnięcia* ……..……..

Odwołano, dnia …….

……

podpis osoby uprawnionej do odwołania upoważnienia

* Data rozwiązania stosunku pracy/umowy cywilnoprawnej