Polityka bezpieczeństwa

I. Informacje ogólne

§ 1

1. Celem niniejszej Polityki Bezpieczeństwa jest zapewnienie zgodności działań firmie **TAUROGIŃSKI JAROSŁAW WOJCIECH UL. Górnicza 6, 59-900 Zgorzelec, NIP 615-103-46-55** z regulacjami prawnymi dotyczącymi zasad bezpieczeństwa przetwarzania danych osobowych.

2. Dokument Polityki Bezpieczeństwa został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:

- Rozporządzeniu 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 [rozporządzenie ogólne o ochronie danych];

- Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (U. 2004 nr 100 poz. 1024)

3. Ochrona danych realizowana jest poprzez zastosowanie odpowiednich środków organizacyjnych i ochrony fizycznej.

4. Obszarem przetwarzania danych firmy:

TAUROGIŃSKI JAROSŁAW WOJCIECH
UL. Górnicza 6
59-900 Zgorzelec,
NIP 615-103-46-55

jest stacja obsługi Renault należąca do firmy, której siedziba znajduje się pod adresem: ul. Górnicza 6, 59-900 ZGORZELEC**,** oraz siedziby podmiotów, którym powierzane są dane osobowe na zasadzie zawartej umowy.

5. Bezpieczeństwo przetwarzania danych osobowych w firmie **TAUROGIŃSKI JAROSŁAW WOJCIECH UL. Górnicza 6, 59-900 Zgorzelec, NIP 615-103-46-55** rozumie się jako powzięcie koniecznych środków w celu zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie.
6. Podjęte zabezpieczenia mają służyć zagwarantowaniu osiągnięcia następujących założeń:

- Poufność danych – zapewnienie, że dane nie zostaną udostępnione nieupoważnionym osobom i podmiotom,
- Integralność danych – zapewnienie, że dane będą przechowywane w sposób uniemożliwiający ingerencję w ich zapis lub ich utratę przez nieuprawnione działania osób trzecich lub zaniedbania,
- Dostępność danych – zapewnienie dostępu do danych i możliwości ich wykorzystania w założonym czasie przez uprawniony podmiot,
- Rozliczalność danych – zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
- Autentyczność danych – zapewnienie, że stan danych jest zgodny z tym, jaki jest deklarowany,
- Integralność systemu – zapewnienie nienaruszalności systemu i dokonywania na nim przypadkowych lub celowych manipulacji,
- Zarządzanie ryzykiem – zapewnienie odpowiedniej kontroli nad procesami dotyczącymi

Renault Serwis "Taurogiński"

przetwarzania danymi osobowymi w celu bieżącego monitorowania i identyfikowania ryzyka dotyczącego bezpieczeństwa, oraz zapewniania jak najlepszych środków w celu minimalizacji możliwych przyszłych szkód.

7. Administrator Danych Osobowych przetwarza dane osobowe w następujących celach:

   I) wykonania umowy kupna-sprzedaży– przetwarzanie jest niezbędne do wykonania umowy, aż do czasu zakończenia umowy,
   II) przygotowania oferty, negocjacji, zawarcia i wykonania umowy,
   III) marketingowych,
   IV) finansowo-księgowych – przetwarzanie jest niezbędne do wykonania przepisów prawa podatkowego,
   V) dane osobowe, które przekazują klienci Administratorowi w celu uzyskania faktury są zamieszczane na fakturach, których kopie przechowuje Administrator przez okres wymagany prawem, podstawą prawną przetwarzania tych danych są przepisy prawa podatkowego. Podanie danych jest dobrowolne , ale konieczne do otrzymania faktury
   VI) obrony przed roszczeniami i dochodzenia roszczeń – do czasu wygaśnięcia okresu roszczeń zgodnie z przepisami Kodeksu Cywilnego,
   VII) prowadzenia procesów reklamacyjnych
   VIII) w celu wypełnienia obowiązków pracodawcy w zakresie zatrudnienia pracowników
   IX) w celu zapewnienie bezpieczeństwa osób oraz mienia znajdujących się w sklepie poprzez stosowanie monitoringu wizyjnego.

8. Szczegóły dotyczące przetwarzania danych w ramach poszczególnych zbiorów znajdują się w opisie tychże zbiorów stanowiących załącznik nr 1 do niniejszej polityki.

II. Definicje

§2

1. Przez użyte w Polityce Bezpieczeństwa określenia należy rozumieć:

1) **Polityka Bezpieczeństwa** – rozumie się przez to Politykę Bezpieczeństwa Ochrony Danych Osobowych stosowaną w firmie **TAUROGIŃSKI JAROSŁAW WOJCIECH UL. Górnicza 6, 59-900 Zgorzelec, NIP 615-103-46-55**

2) **Administrator Danych Osobowych –** Administratorem Danych Osobowych w rozumieniu niniejszej Polityki Bezpieczeństwa jest firma **TAUROGIŃSKI JAROSŁAW WOJCIECH**

3) **Firma -** TAUROGIŃSKI JAROSŁAW WOJCIECH UL. Górnicza 6, 59-900 Zgorzelec, NIP 615-103-46-55

4) **Rozporządzenie** – rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) z późniejszymi zmianami;

5) **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 [rozporządzenie ogólne o ochronie danych]

6) **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do

Renault Serwis - Taurogiński

zidentyfikowania osoby fizycznej;

7) **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw jest rozproszony lub podzielony funkcjonalnie

8) **Usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dotyczą.

9) **Przetwarzanie danych** – rozumiane jako wykonywanie jakichkolwiek operacji na danych osobowych, takich jak np. zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie;

10) **System monitorujący** – zestaw kamer wraz z urządzeniem rejestrującym;

11) **Użytkownik** - to upoważniony przez administratora danych osobowych pracownik, zleceniobiorca, wykonawca umowy o dzieło, wykonawca umowy o świadczenie usług, praktykant lub stażysta wyznaczony do przetwarzania danych osobowych; użytkownikiem może być również administrator danych osobowych,

III. Zakres zastosowania Polityki Bezpieczeństwa

§ 3

1. Polityka bezpieczeństwa zawiera informacje dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych, mających na celu zapewnienie należytej ochrony przetwarzanych danych osobowych;

§ 4

Politykę bezpieczeństwa stosuje się przed wszystkim do:

1) wszystkich informacji dotyczących danych osobowych podmiotów oraz osób współpracujących z Administratorem
2) wszystkich informacji dotyczących danych osobowych zleceniodawców i klientów
3) informacji dotyczących zabezpieczenia danych osobowych w systemach tradycyjnych – papierowych
4) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych,
5) rejestru osób dopuszczonych do przetwarzania danych osobowych,
6) innych dokumentów zawierających dane osobowe.

§ 5

Zakres ochrony danych osobowych określony w Polityce Bezpieczeństwa ma zastosowanie do systemów informatycznych, a w szczególności do:

1. Wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie.
2. Wszystkich lokalizacji - pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.
3. Wszystkich pracowników, zleceniobiorców, wykonawców umów o dzieło, umów o świadczenie usług, praktykantów i stażystów na rzecz Administratora Danych

Osobowych, które uzyskały od niego upoważnienie do przetwarzania danych osobowych lub mają dostęp do danych osobowych podlegających ochronie.

IV. Obowiązki i odpowiedzialność

§ 6

Do najważniejszych obowiązków Administratora Danych należy:

1. Zastosowanie odpowiedniej organizacji w celu zapewnienia należnej ochrony danych osobowych zgodnie z obowiązującymi regulacjami prawnymi.
2. Zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki Bezpieczeństwa.
3. Udzielanie upoważnień do przetwarzania danych osobowych oraz ich anulacja.
4. Zapewnienie szkoleń użytkownikom przed dopuszczeniem ich do pracy z systemem informatycznym przetwarzającym dane osobowe.
5. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.
6. Podjęcie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych.
7. Sprawowanie nadzoru nad bezpieczeństwem danych osobowych.
8. Czuwanie nad tym, by użytkownicy stosowali odpowiednie procedury zgodne z zasadami ochrony danych osobowych.
9. Monitorowanie możliwych zagrożeń dotyczących przetwarzania danych oraz bieżące dostosowywanie odpowiednich środków w zakresie doskonalenia ochrony danych osobowych;
10. Kontrola działania systemu tradycyjnego oraz podejmowanie działań gwarantujących zapewnienie ciągłości ich poprawnego funkcjonowania.
11. Zapewnienie środków mających zabezpieczyć próby naruszenia bezpieczeństwa informacji;
12. Dostosowywanie procedur bezpieczeństwa i standardów zabezpieczeń;
13. Zarządzanie licencjami oraz procedurami ich dotyczącymi;

§ 7

Do obowiązków osób upoważnionych do przetwarzania danych osobowych należy:

1. Zapoznanie się z obowiązującą Polityką Bezpieczeństwa i stosowanie jej w jak najszerszym zakresie w celu zapewnienia ochrony danych osobowych.
2. Zachowanie w tajemnicy swoich identyfikatorów oraz haseł do systemu monitorującego.
3. Przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami.
4. Działanie zgodnie z ustalonymi regulacjami wewnętrznymi dotyczącymi przetwarzania danych osobowych.
5. Zachowanie w tajemnicy danych osobowych, do których uzyskały dostęp.
6. Zapewnienie ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem.

Renault-Serwis-Taurogiński

7. Zgłaszanie Administratorowi Danych Osobowych wszelkich podejrzeń naruszenia lub stwierdzonych naruszeń oraz słabości systemu przetwarzającego dane osobowe.

V. Zarządzanie ochroną danych osobowych

§ 8

Za ochronę danych osobowych firmy **TAUROGIŃSKI JAROSŁAW WOJCIECH UL. Górnicza 6, 59-900 Zgorzelec, NIP 615-103-46-55** odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z upoważnieniem oraz rolą sprawowaną w procesie przetwarzania danych.

1. Dostęp do danych osobowych powinien być przyznawany zgodnie z zasadą wiedzy koniecznej.

2. Użytkownik, mający styczność z danymi osobowymi, jest zobowiązany do stosowania odpowiednich środków ochrony danych osobowych oraz do przetwarzania danych w granicach udzielonego mu upoważnienia.

3. Należy zagwarantować poufność, integralność i rozliczalność przetwarzanych danych osobowych.

4. Należy zapewnić adekwatny do zmieniających się warunków poziom bezpieczeństwa przetwarzanych danych osobowych.

5. Dane osobowe należy chronić przed nieuprawnionym dostępem, modyfikacją lub zniszczeniem.

6. Operacje na danych osobowych należy prowadzić wyłącznie za pomocą autoryzowanych urządzeń służbowych.

7. Administrator Danych Osobowych dopuszcza do przetwarzania danych osobowych tylko osoby, którym wcześniej udzielił upoważnienia na mocy art. 29 RODO.

VI. Szkolenia użytkowników

§ 9

1. Każdy użytkownik powinien zostać poddany szkoleniu w zakresie ochrony danych osobowych w systemie informatycznym i tradycyjnym przed dopuszczeniem do pracy w systemie danych osobowych firmy **TAUROGIŃSKI JAROSŁAW WOJCIECH UL. Górnicza 6, 59-900 Zgorzelec, NIP 615-103-46-55.**

2. Za przeprowadzenie szkolenia odpowiada Administrator Danych Osobowych.

3. Szkolenie powinno obejmować przepisy dotyczące ochrony danych osobowych, wydane na ich podstawie akty wykonawcze, Politykę Bezpieczeństwa.

4. Każdy użytkownik, po zapoznaniu się z prawnymi wytycznymi oraz Polityką bezpieczeństwa, a przed dopuszczeniem do przetwarzania danych, powinien zobowiązać się do ich przestrzegania przez podpisanie **Oświadczenia użytkownika.**

VII. Upoważnienie do przetwarzania danych osobowych

Ronald Taurogiński

§ 10

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie wydane przez Administratora Danych na mocy art. 29 RODO.

2. Upoważnienia są wydawane po dobyciu niezbędnego szkolenia z ochrony danych osobowych, przed rozpoczęciem przetwarzania danych osobowych.

3. Użytkownik otrzymuje upoważnienia do przetwarzania danych osobowych od Administratora Danych Osobowych po dostarczeniu podpisanego oświadczenia.

4. Administrator Danych Osobowych upoważnia Użytkownika do przetwarzania danych osobowych na podstawie otrzymanego **Oświadczenia** (stanowiącego załącznik **5 do Polityki Bezpieczeństwa**) poprzez wydanie **Upoważnienia do przetwarzania danych osobowych** sporządzane wg wzoru stanowiącego załącznik **nr 4 do Polityki Bezpieczeństwa**.

5. Upoważnienie do przetwarzania danych może być w każdym czasie odwołane przez Administratora Danych Osobowych. **Oświadczenie o odwołaniu upoważnienia** powinno być sporządzone na piśmie stanowiącego załącznik **nr 6 do Polityki Bezpieczeństwa**.

6. Upoważnienie do przetwarzania danych osobowych wygasa z chwilą ustania przesłanki będącej podstawą wydania upoważnienia, w tym w szczególności wygaśnięcia stosunku pracy lub umowy cywilnoprawnej łączącej Użytkownika z Administratorem Danych Osobowych.

VIII. Ewidencja osób upoważnionych

§ 11

1. Administratora Danych zobowiązany jest do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych w firmie.
2. **Ewidencja osób upoważnionych** prowadzona jest według wzoru dokumentu, stanowiącego **załącznik do Polityki Bezpieczeństwa nr 2.**

IX. Udostępnianie danych osobowych

§ 12

1. Dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa oraz osobom, których dotyczą.

2. Do udostępnienia danych osobowych konieczna jest zgoda Administratora Danych Osobowych.

3. Wszelkie informacje, zawierające dane osobowe, powinny być przekazywane uprawnionym podmiotom lub osobom listem poleconym za potwierdzeniem odbioru lub innym bezpiecznym sposobem, zgodnym z aktualnym wymogiem prawnym lub umową.

4. W chwili udostępniania danych osobowych, należy poinformować, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

Renault Serwis Puroński

X. Wymagania bezpieczeństwa

§ 13

1. Dane osobowe w postaci tradycyjnej (papierowej) mogą być przetwarzane wyłącznie w obszarze przetwarzania danych osobowych, na które składa się pomieszczenie biura w stacji obsługi Renault w Zgorzelcu przy ul. Górniczej 6, za wyjątkiem sytuacji udostępnienia danych osobowych lub powierzenia przetwarzania danych osobowych innym podmiotom na podstawie Umowy powierzenia danych osobowych. **Wykaz pomieszczeń, tworzących obszar przetwarzania danych osobowych**, znajduje się w **załączniku nr 3** do Polityki Bezpieczeństwa.
2. Dane osobowe przetwarzane są przez firmę TAUROGIŃSKI JAROSŁAW WOJCIECH UL. Górnicza 6, 59-900 Zgorzelec, NIP 615-103-46-55 z zastosowaniem zabezpieczeń ochrony danych w postaci środków organizacyjnych, technicznych i środków ochrony fizycznej.
3. Dla zapewnienia poufności, rozliczalności i integralności przetwarzanych danych stosuje się następujące środki:

A. Środki organizacyjne:

- wdrożenie Polityki bezpieczeństwa przetwarzania danych osobowych
- wdrożenie Instrukcji zarządzania systemem informatycznym
- ustalenie odpowiedniej procedury udzielania upoważnień przez Administratora Danych po uprzednim przeszkoleniu przyszłych użytkowników warsztatu
- prowadzenie Ewidencji osób uprawnionych do przetwarzania danych osobowych
- ustalona procedura postępowania w sytuacji naruszenia ochrony danych osobowych
- wprowadzenie wymagalności składania deklaracji poufności przez Użytkowników danych
- wprowadzenie procedur przechowywania danych

B. Środki techniczne:

- zbiory danych osobowych przetwarzane są wyłącznie na sprzęcie służbowym
- komputery wyposażone są w ochronę antywirusową
- dostęp do komputerów wymaga uwierzytelnienia poprzez podanie hasła i identyfikatora
- w komputerach zastosowano wygaszacze ekranu oraz tryb uśpienia po około 15 minutach bezczynności sytemu

C. Środki ochrony fizycznej:

- pomieszczenia, w których przechowywane są dane osobowe, zamykane są na klucz a dostęp do nich odbywa się wyłącznie w obecności Administratora i upoważnionych pracowników warsztatu
- w budynku zainstalowany jest alarm
- Warsztat jest pod ochroną firmy ochroniarskiej Piast
- Budynek jest pod stałym monitoringiem z zewnątrz
- monitoringowi podlegają również pomieszczenia warsztatu w celu zapewnienia bezpieczeństwa i zabezpieczenia mienia klienta
- zbiór danych osobowych w formie papierowej przechowywany jest w zamkniętych

Renault-Serwis Taurogiński

szafkach, w pomieszczeniu biurowym, zamykanym na klucz, do którego dostęp mają osoby upoważnione.

- kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej szafie, w wyznaczonym do tego miejscu

XI. Kontrola stanu systemu ochrony danych osobowych

§ 14

1. Administrator Danych Osobowych raz w roku sprawdza zgodność procedur przetwarzania danych osobowych, stosowanych w serwisie samochodowym, z przepisami o ochronie danych osobowych i przygotowuje odpowiednie sprawozdanie z kontroli

XII. Dokonanie obowiązku informacyjnego

§ 15

Podczas zbierania danych osobowych od osoby, której one dotyczą, w wypadkach przewidzianych RODO należy poinformować tę osobę o:

1. Nazwie Administratora Danych, jego siedzibie i sposobie kontaktu.
2. Celu zbierania danych, a w szczególności o przewidywanych odbiorcach lub kategoriach odbiorców danych.
3. Prawie dostępu do swoich danych, do ich poprawiania, możliwości żądania ich usunięcia, wniesienia skargi do organu nadzorczego.
4. Czasie przetwarzania danych.
5. Dobrowolności lub obowiązku podania danych. W przypadku, gdy podanie danych jest konieczne, powołanie się na podstawę prawną.

XIII. Postępowanie w sytuacji naruszenia bezpieczeństwa danych osobowych

§ 16

1. Każdy użytkownik zobowiązany jest poinformować Administratora Danych Osobowych o stwierdzeniu zagrożenia lub naruszenia zasad ochrony danych osobowych.
2. Do typowych zagrożeń bezpieczeństwa należy zaliczyć:

- nieodpowiednie zabezpieczenie pomieszczeń, urządzeń i dokumentów
- niewłaściwe zabezpieczenie sprzętu komputerowego i oprogramowania przed zniszczeniem lub dostępem niepowołanych osób
- łamanie procedur ochrony danych osobowych ustalonych w Polityce Bezpieczeństwa przez Użytkowników

3. Do typowych incydentów bezpieczeństwa danych osobowych należą:

Renault-Serwis-Tauroński

- zdarzenia losowe zewnętrzne: zalanie wodą, pożar obiektu, utrata zasilania, utrata łączności
- zdarzenia losowe wewnętrzne: usterka komputerów, awaria serwera, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata lub zagubienie danych
- umyślne incydenty: włamanie do systemu informatycznego lub pomieszczeń, działanie wirusów i innego szkodliwego oprogramowania, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych

4. W przypadku stwierdzenia zagrożenia ochrony danych osobowych Administrator Danych prowadzi postępowanie wyjaśniające w zakresie którego:

- określa przyczyny i zakres powstałego zagrożenia oraz jego ewentualne skutki
- inicjuje ewentualne działania dyscyplinarne
- planuje wprowadzenie działań, zmierzających do eliminacji podobnych zagrożeń w przyszłości
- przygotowuje sprawozdanie z przeprowadzonych działań

5. W przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych, Administrator Danych prowadzi postępowanie wyjaśniające, w zakresie którego:

- ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały
- zabezpiecza dowody
- ustala osoby odpowiedzialne za naruszenie
- podejmuje działania mające na celu usunięcie skutków incydentu i ograniczenia szkód
- w razie potrzeby inicjuje działania dyscyplinarne
- dokonuje analizy incydentu i rekomenduje działania, mające na celu eliminację podobnych incydentów w przyszłości
- dokumentuje prowadzone postępowania zgodnie ze wzorem Raportu z naruszenia bezpieczeństwa danych osobowych stanowiących załącznik nr 7 do Polityki Bezpieczeństwa.

XIV. Aktualność Polityki Bezpieczeństwa

§ 17

1. Polityka bezpieczeństwa serwisu samochodowego powinna być regularnie sprawdzana pod kątem zgodności z obowiązującym prawem oraz obecnym stanem struktury i zasad funkcjonowania serwisu. W razie potrzeby powinna być aktualizowana stosownie do zmian w systemie prawnym oraz w funkcjonowaniu serwisu.

Renault-Serwis-"Tarogiński"

XV. Postanowienia końcowe

§ 18

1. Do obowiązków Administratora Danych należy zapoznanie każdego Użytkownika z treścią Polityki Bezpieczeństwa.

2. Wszyscy Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych procedur zawartych w Polityce.

3. W przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego podejrzenia takiego incydentu, wobec osoby, która nie podjęła w związku z tym odpowiednich działań, zgodnych z Polityką a w szczególności nie powiadomiła Administratora Danych Osobowych lub też nie podjęła działań dokumentujących i zabezpieczających okoliczności zdarzenia, dopuszcza się możliwość podjęcia działań dyscyplinarnych.

4. Orzeczona kara dyscyplinarna wobec osoby, która nie dopełniła powyższych obowiązków, nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z RODO oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

5. W sprawach nieuregulowanych w niniejszej Polityce zastosowanie mają przepisy RODO oraz rozporządzenia.

Renault-Serwis-"Taurogiński"