Polityka Ochrony Danych Osobowych

1. Polityka Ochrony Danych Osobowych, zwana dalej „Polityką”, określa środki techniczne i organizacyjne zastosowane przez administratora danych dla zapewnienia ochrony danych osobowych oraz tryb postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych w systemie informatycznym lub w kartotekach, albo w sytuacji podejrzenia takiego naruszenia.
2. Celem niniejszej Polityki jest wypełnienie założeń Rozporządzenia 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 (ogólne rozporządzenie o ochronie danych zwane dalej w skrócie – „RODO”).
3. Nadzór nad przestrzeganiem zasad opisanych w niniejszej Polityce oraz przepisów ochrony danych osobowych pełni Właściciel. Zobowiązuje on wszystkich pracowników i współpracowników do zapoznania się z Polityką Ochrony Danych Osobowych oraz do bezwzględnego przestrzegania zawartych w niej zasad.
4. Definicje i załączniki:
    1) administrator danych – podmiot (osobę fizyczną lub prawną), który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych, jest nim Total Project Management S.C. A. Członka K. Członka z siedzibą przy ul. Topolowej 11, Kawęczynek, 05-220 Konstancin-Jeziorna prowadząca działalność hotelową pod nazwą Patchwork Warsaw Hostel przy ul. Chmielnej 5/7 w Warszawie, reprezentowana przez p. Alinę Członka,
    2) bezpieczeństwo informacji – zachowanie poufności, integralności i dostępności informacji; dodatkowo pod tym pojęciem mogą być brane pod uwagę takie własności jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność,
    3) dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,
    4) dane szczególne – 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, dane dotyczące zdrowia, seksualności lub orientacji seksualnej,
    5) incydent ochrony danych osobowych – zdarzenie albo seria niepożądanych lub niespodziewanych zdarzeń ochrony danych osobowych stwarzających znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrożenia ochrony danych osobowych,
    6) naruszenie ochrony danych osobowych – naruszenie bezpieczeństwa prowadzące do przypadkowego lub celowego zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych,

Procedura postępowania administratora w przypadku naruszenia ochrony danych stanowi załącznik nr 1 do niniejszej Polityki,

7) obszar przetwarzania danych – budynki i pomieszczenia określone przez administratora danych, w których przetwarzane są dane osobowe i inne informacje prawnie chronione,
8) osoba, podmiot danych – osoba, której dane dotyczą,
9) odbiorca danych – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe (z wyjątkiem organów, które wg prawa mogą otrzymywać dane osobowe w ramach konkretnego postępowania),
10) podmiot przetwarzający – osoba fizyczna lub prawna, której administrator danych powierzył przetwarzanie danych osobowych,
11) postępowanie z ryzykiem – proces planowania i wdrażania działań wpływających na ryzyko; ryzyko – niepewność osiągnięcia zamierzonych celów, szacowanie ryzyka – proces identyfikowania, analizowania i oceniania ryzyka,
12) poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom,
13) profilowanie – dowolna forma 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,
14) serwisant – osoba lub firma zajmująca się sprzedażą, instalacją, naprawą i konserwacją sprzętu użytkowanego przez administratora danych,
15) system informatyczny – sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny a system ten tworzy sieć teleinformatyczną administratora danych,
16) teletransmisja – przesyłanie informacji za pośrednictwem publicznej sieci telekomunikacyjnej czyli internetu,
17) uwierzytelnienie – działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby,
18) użytkownik – osoba upoważniona do przetwarzania danych osobowych, której nadano identyfikator i hasło,
19) identyfikator – ciąg znaków identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
20) hasło – ciąg znaków znany jedynie użytkownikowi,
21) zgoda osoby, której dane dotyczą – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania, przyzwala na przetwarzanie dotyczących jej danych osobowych.

5. W celu zwiększenia efektywności ochrony danych osobowych łączy się różne zabezpieczenia. Ochrona danych osobowych jest realizowana poprzez zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe oraz przez użytkowników.
6. Zastosowane zabezpieczenia służą osiągnięciu poniższych celów:

1) rozliczalność – właściwość zapewniająca, że działania użytkownika mogą być przypisane w sposób jednoznaczny tylko temu użytkownikowi,
2) integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
3) poufność danych – właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
4) integralność systemu – właściwość systemu, wykluczająca ingerencję przez osoby nieupoważnione.

7. Realizację powyższych celów powinny zagwarantować następujące założenia:
   1) wdrożenie procedur określających postępowanie osób dopuszczonych do przetwarzania danych osobowych oraz ich odpowiedzialność za ochronę tych danych,
   2) przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych,
   3) przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (identyfikatory i hasła),
   4) podejmowanie niezbędnych działań w celu likwidacji słabych ogniw w systemie zabezpieczeń,
   5) okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych.
8. Dla zapewnienia bezpieczeństwa danych i informacji zastosowano następujące środki organizacyjne:
   1) każda osoba działająca z upoważnienia administratora danych i mająca dostęp do danych osobowych przetwarzała je wyłącznie na polecenie administratora danych,
   2) każdy z pracowników i współpracowników powinien zachować szczególną ostrożność przy przenoszeniu danych,
   3) należy chronić dane przed dostępem do nich osób nieupoważnionych,
   4) pomieszczenia, w których są przetwarzane dane osobowe powinny być zamykane na klucz,
   5) dostęp do kluczy posiadają tylko upoważnieni pracownicy i współpracownicy,
   6) dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W wypadku gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie zezwolenia administratora danych,
   7) dostęp do pomieszczeń, w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy,
   8) w przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym do wykonania niezbędnych czynności,
   9) szafy, w których przechowywane są dane powinny być zamykane na klucz,
   10) klucze do tych szaf posiadają tylko upoważnieni pracownicy,
   11) szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych, a następnie powinny być zamykane,
   12) dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych, a następnie muszą być chowane do szaf,
   13) dostęp do komputerów, na których są przetwarzane dane, mają tylko upoważnieni pracownicy i współpracownicy,

14) monitory komputerów, na których przetwarzane są dane, są tak ustawione, aby osoby nieupoważnione nie miały wglądu w dane,
15) w wypadku potrzeby wyniesienia komputera przenośnego zawierającego dane osobowe, lub inne informacje chronione, komputer taki musi być odpowiednio zabezpieczony. Osoba dysponująca tym komputerem jest zobowiązana szczególnie dbać o jego bezpieczeństwo i nie udostępniać osobom nieupoważnionym,
16) w przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności,
17) nośniki do tego użyte należy wyczyścić, aby nie zostały na nich dane osobowe,
18) w wypadku niemożliwości skasowania danych z nośnika (np. płyta cd/dvd) należy nośnik zniszczyć fizycznie,
19) niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną,
20) sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz,
21) błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający ich odtworzenie.

9. Za naruszenie ochrony danych osobowych uważa się w szczególności:
   1) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują, w tym włamanie lub jego usiłowanie,
   2) naruszenie lub próby naruszenia integralności danych rozumiane jako wszelkie modyfikacje, zniszczenia lub próby ich dokonania przez osoby nieuprawnione lub uprawnione działające w złej wierze lub jako błąd w działaniu osoby uprawnionej (np. zmianę zawartości danych, utratę całości lub części danych),
   3) naruszenie lub próby naruszenia integralności systemu informatycznego, w tym zniszczenie, uszkodzenie, próby nieuprawnionej ingerencji zmierzające do zakłócenia jego działania bądź pozyskania zawartych w nim danych w sposób niedozwolony lub w celach niezgodnych z przeznaczeniem danych,
   4) ujawnienie metod pracy lub sposobu działania systemu informatycznego,
   5) zmianę lub utratę danych zapisanych na kopiach zapasowych,
   6) naruszenie lub próby naruszenia poufności danych,
   7) nieuprawniony dostęp (nielegalne logowanie lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
   8) inny stan systemu informatycznego lub pomieszczeń, niż pozostawiony przez użytkownika po zakończeniu pracy
10. O możliwym naruszeniu bezpieczeństwa danych mogą świadczyć w szczególności inne niż zwykle – nietypowe:
   1) stan zabezpieczeń i działanie systemu informatycznego,
   2) stan komputerów i innych urządzeń,
   3) stan pomieszczeń,
   4) zawartość zbioru danych,
   5) zachowanie innych pracowników,
   5) obecność osób nieznajomych w miejscach, w których są przetwarzane dane,
   6) inne nietypowe zdarzenia i sytuacje.
11. Osoba, która stwierdziła naruszenie bezpieczeństwa danych lub ma podejrzenie, że takie naruszenie mogło nastąpić powinna niezwłocznie:
   1) powiadomić o tym administratora danych,

2) podjąć czynności zmierzające do powstrzymania dalszego zagrożenia dla danych,
3) zabezpieczyć dowody umożliwiające ustalenie przyczyn i skutków naruszenia.

12. Wobec osoby, która w przypadku naruszenia zabezpieczeń bezpieczeństwa danych lub uzasadnionego podejrzenia takiego naruszenia nie podjęła działań określonych w niniejszym dokumencie, w szczególności nie powiadomiła administratora danych, wszczyna się postępowanie dyscyplinarne lub porządkowe.
13. Na obszar, w którym są przetwarzane dane składają się Biuro i Recepcja Hostelu.
14. Administrator przy przetwarzaniu danych korzysta z usług podmiotów zewnętrznych, którym może udostępniać dane w celu realizacji swojej działalności, w szczególności świadczenia usług turystycznych i noclegowych. Z podmiotami tymi posiada podpisane umowy zobowiązujące do przetwarzania powierzonych danych z zachowaniem zasad wymaganych przepisami prawa. Do podmiotów tych należą:
    1) IT Omega,
    2) biuro rachunkowe.
15. Dostęp do danych osobowych:
    1) Przetwarzanie, w tym udostępnianie danych osobowych jest prawnie dopuszczalne, jeżeli jest niezbędne dla zrealizowania obowiązków wynikających z przepisów prawa.
    2) W przypadku udostępnienia danych osobowych administrator danych udostępnia posiadane informacje osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
    3) Dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
    4) Podmiot występujący o udostępnienie informacji powinien wskazać podstawę prawną upoważniającą go do otrzymania tych danych albo uzasadnioną potrzebę żądania ich udostępnienia. Tylko w takiej sytuacji można dokonać oceny, czy w określonym przypadku udostępnienie danych jest prawnie dopuszczalne.
    5) Przetwarzanie, w tym udostępnianie danych osobowych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje w celu badań naukowych, dydaktycznych, historycznych oraz statystycznych.
    6) Udostępnienie danych może nastąpić jedynie za zgodą administratora danych i powinno być odpowiednio udokumentowane.
16. Prawa podmiotów danych.
    Każdej osobie, której dane osobowe są przetwarzane przysługuje prawo do kontroli przetwarzania jej danych osobowych, a w szczególności prawo do:
    1) uzyskania wyczerpującej informacji, czy jej dane osobowe są przetwarzane oraz do otrzymania informacji o pełnej nazwie i adresie siedziby administratora danych;
    2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych osobowych;
    3) uzyskania informacji, od kiedy są przetwarzane jej dane osobowe, oraz podania w powszechnie zrozumiałej formie treści tych danych;
    4) uzyskania informacji o źródle, z którego pochodzą dane osobowe jej dotyczące;
    5) uzyskania informacji o sposobie udostępniania danych osobowych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym te dane osobowe są udostępniane;
    6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one

niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem przepisów prawa albo są już zbędne do realizacji celu, dla którego zostały zebrane.

17. Niniejsza Polityka jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym.
18. Pracownik lub współpracownik zobowiązany jest złożyć oświadczenie o tym, iż został zapoznany z przepisami dotyczącymi ochrony danych osobowych oraz z niniejszą Polityką, i zobowiązuje się do ich przestrzegania.
19. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie aktualnie obowiązujące przepisy prawa w zakresie ochrony danych osobowych.

Zatwierdzam

.....
(data, podpis, pieczęć
administratora danych)

Załącznik nr 1

Procedura postępowania w przypadku naruszenia ochrony danych osobowych dla administratora.

1. Administrator po uzyskaniu informacji o możliwym naruszeniu ochrony danych:
   1) zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając stopień zagrożenia bezpieczeństwa danych,
   2) odbiera dokładną relację ze zdarzenia od osoby powiadamiającej oraz od innych osób, mogących posiadać istotne informacje w sprawie,
   3) nawiązuje kontakt ze specjalistami zewnętrznymi, jeśli zachodzi taka potrzeba, w celu usunięcia skutków naruszenia,
   4) analizuje zaistniałe naruszenie i podejmuje działania naprawcze oraz zmiany techniczne i organizacyjne w celu zapobieżenia podobnej sytuacji w przyszłości.
2. Administrator dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając z niego Raport, którego wzór stanowi załącznik nr 1a.
3. Administrator prowadzi Rejestr naruszeń, którego wzór stanowi załącznik nr 1b.
4. Administrator zgłasza Prezesowi Urzędu Ochrony Danych Osobowych przypadek naruszenia ochrony danych osobowych w ciągu 72 godzin od jego stwierdzenia, chyba że jest mało prawdopodobne, by skutkowało ono naruszeniem ryzykiem naruszenia praw lub wolności osób fizycznych (formularz zgłoszenia dostępny na stronie urzędu).
5. Administrator niezwłocznie, w sposób jasny i prosty, zawiadamia osoby, których dane dotyczą, o zaistniałym naruszeniu bezpieczeństwa ich danych, jeśli może ono powodować wysokie ryzyko naruszenia praw lub wolności tych osób.

Załącznik nr 1a

RAPORT NR 1/2018 Z NARUSZENIA OCHRONY DANYCH

1. Data ..... Godzina ..... wystąpienia naruszenia lub jego zauważenia*

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem

   .....
   (imię, nazwisko, stanowisko służbowe,):

3. Lokalizacja zdarzenia .....
   (określenie pomieszczenia, kartoteki, komputera, programu, bazy danych):

4. Opis naruszenia i jego okoliczności:

   .....

   .....

5. Działania podjęte po naruszeniu:

   .....

   .....

6. Wstępna ocena przyczyn wystąpienia naruszenia:

   .....

7. Postępowanie wyjaśniające i naprawcze:

   .....

   .....

   .....

....
(podpis pracownika) (data i podpis administratora)

Załącznik nr 1b

REJESTR NARUSZEŃ BEZPIECZEŃSTWA DANYCH ORAZ DZIAŁAŃ KORYGUJĄCYCH I ZAPOBIEGAWCZYCH

Numer naruszenia	**Opis naruszenia**	**Źródło zgłoszenia** (***zawiadomienie, kontrola, itd.***)	**Data rozpoczęcia**	**Data zakończenia**	**Odpowiedzialny za realizację**	**Przyczyna naruszenia**	**Działanie zapobiegawcze i korygujące**	**Ocena skuteczności**