ZASADY BEZPIECZEŃSTWA W LOYALTY PARTNER POLSKA SP. Z O.O.

Wstęp

Niniejszy dokument powstał w oparciu o zapisy zawarte w polityce bezpieczeństwa Loyalty Partner Polska Sp. z o.o. oraz te pochodzące z regulaminu użytkowania systemu IT (dokument „IT Terms of Use" dostępny w intranecie LP). Jego celem jest wyznaczenie standardów postępowania podczas użytkowania infrastruktury LP (w szczególności jak bezpiecznie korzystać z poczty e-mail, sieci, sprzętu komputerowego) oraz określenie podstawowych zasad na jakich przetwarzane/udostępniane są dane osobowe.

Administrator Danych Osobowych, Inspektor Ochrony Danych Osobowych

Administrator Danych Osobowych („ADO")– podmiot lub osoba, które decydują o celach i środkach przetwarzania danych osobowych. Przez ADO rozumie się **Loyalty Partner Polska Sp. z o.o. („LP")**.

Inspektor Ochrony Danych („**IOD**") – osoba wyznaczona przez ADO, która jest odpowiedzialna za zapewnienie przetwarzania danych zgodnie z odpowiednimi przepisami ustawy i prawa. W Loyalty Partner Polska Sp. z o.o. funkcję IOD pełni **Dariusz Sadowski** (mojedane@payback.net / dariusz.sadowski@payback.net).

LP wyznaczył i zgłosił do rejestru prowadzonego przez Urząd Ochrony Danych Osobowych IOD, który jest odpowiedzialny za nadzorowanie i weryfikowanie czy przetwarzanie danych przez ADO i jego pracowników jest zgodne przepisami o ochronie danych osobowych, w tym Ogólnego Rozporządzenia o Ochronie Danych Osobowych („**RODO**"), przepisów krajowych oraz wewnętrznymi politykami ADO

IOD w szczególności:

- informuje ADO, podmioty przetwarzające dane osobowe w imieniu ADO oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów o ochronie danych osobowych i doradza im w tym zakresie.
- monitoruje przestrzeganie przepisów o ochronie danych osobowych oraz polityk ADO lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
- współpracuje z organem nadzorczym (prezesem Urzędu Ochrony danych Osobowych);
- pełnieni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym prowadzonymi przez ADO konsultacjami
- nadzorowanie kto ma dostęp do danych osobowych (zarówno w ramach organizacji ADO oraz przez podmioty zewnętrzne);
- określa środki bezpieczeństwa niezbędne do zapewnienia przestrzegania przepisów o ochronie danych osobowych;
- definiuje wymagania związane z wymianą danych z podmiotami zewnętrznymi;
- prowadzi okresowe audyty stanu bezpieczeństwa (zarówno w ramach organizacji ADO oraz w stosunku do podmiotów zewnętrznych);

Zasady przetwarzania danych osobowych w LP

Dane osobowe (eng. **PII data**) – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej: (imię, nazwisko, adres, numer telefonu, adres email, data urodzenia, wykształcenie, zarobki, etc.).

Ponadto z punktu widzenia bezpieczeństwa, do danych o istotnym znaczeniu należą także informacje o numerze karty PAYBACK oraz dane transakcyjne, które w połączeniu z danymi osobowymi również zyskują status danych osobowych.

Szczególne kategorie danych osobowych - dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetycznych, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby.

LP co do zasady nie przetwarza (nie zbiera, nie analizuje, nie wykorzystuje w celach marketingowych) szczególnych kategorii danych osobowych.

Dostęp do danych osobowych:

- Dostęp do danych osobowych powinny mieć jedynie te osoby i tylko w takim zakresie w jakim jest to niezbędne do wykonywania przez nie obowiązków służbowych.
- Upoważnienie do przetwarzania danych osobowych nadaje przedstawiciel Działu HR (w imieniu ADO).
- Osoba upoważniona nie ma prawa do nadawania dalszych upoważnień.
- Upoważnienie określa zakres danych do jakich pracownik ma dostęp.
- Upoważnienie do przetwarzania danych osobowych wygasa z chwilą rozwiązania umowy zawartej przez ADO z osobą, której zostało nadane lub w przypadku gdy zostało nadane na czas określony z upływem czasu na jaki zostało nadane.
- Każdy kto przetwarza dane osobowe obowiązany jest zachować w tajemnicy informacje do których posiada dostęp.
- Podczas przetwarzania danych należy zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem.

Zasady przetwarzania danych osobowych przez podmioty zewnętrzne

Jeżeli przetwarzanie ma być dokonywane w imieniu ADO przez podmioty zewnętrzne, korzysta on wyłącznie z usług takich podmiotów, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

Każdy transfer danych uczestników PAYBACK do podmiotu zewnętrznego (w tym zbieranie takich danych w imieniu LP, dostęp do danych w ramach infrastruktury LP, wykorzystywanie danych w celu świadczenia na rzecz LP usług) musi być zaakceptowany przez IOD. Taka akceptacja poprzedzona jest przeprowadzeniem audytu bezpieczeństwa. W tym celu podmiot zewnętrzny musi wypełnić kwestionariusz bezpieczeństwa dostarczony przez IOD. W przypadku podmiotów mających dostęp do dużej ilości / zakresu danych, IOD może zdecydować o przeprowadzeniu szczegółowego audytu w miejscu prowadzenia działalności / przetwarzania danych przez taki podmiot.

Podstawą do przekazania danych podmiotom zewnętrznym (nie będących administratorami tychże danych) jest umowa powierzenia przetwarzania danych osobowych, w której jest jasno określony:

- cel przekazywania danych (np. w celu wykonania danej umowy, w celu przeprowadzenia akcji marketingowej),
- czynności jakie będą dokonywane z wykorzystaniem danych (np. wprowadzenie do systemu, selekcja, segmentacja danych, przeprowadzenie wysyłki mailingu),
- kategorie podmiotów, których dane dotyczą (Członkowie PAYBACK, pracownicy LP, kontrahenci).
- zakres przekazywanych danych (np. imię, nazwisko, numer karty PAYBACK, numer telefonu),
- okres na jaki podmiot będzie przetwarzał dane
- sposób wymiany danych,
- zasady dalszego powierzania danych przez podmiot zewnętrzny,
- szczegółowe obowiązki podmiotu zewnętrznego
- konsekwencje wynikające z ujawnienia danych osobom nieuprawnionym (np. kara umowna)

Ponadto dla każdego podmiotu zewnętrznego przetwarzającego takie dane wymagane jest określenie miejsca przetwarzania (fizyczny adres gdzie znajdują się serwery, który może różnić się od adresu lokalizacji biura spółki).

Każdy proces pozyskiwania danych osobowych od Członków PAYBACK lub innych podmiotów w imieniu LP przez podmioty zewnętrzne, powinien także uzyskać akceptację IOD. Należy pamiętać, że poza koniecznością prawnego uregulowania takiej aktywności dochodzi jeszcze potrzeba weryfikacji czy zaimplementowane rozwiązanie spełnia techniczne wymogi bezpieczeństwa.

W przypadku jakichkolwiek wątpliwości co do planowanych działań w zakresie przetwarzania danych, należy zwrócić się do IODO z prośbą o rozstrzygnięcie wątpliwości. Przed udzieleniem przez IOD odpowiedzi należy wstrzymać wszystkie działania na danych osobowych, co do których istnieją wątpliwości czy są zgodne z wymaganiami prawnymi oraz technicznymi.

Ogólne warunki użytkowania sprzętu komputerowego i przepisy bezpieczeństwa IT

Środki bezpieczeństwa stosowane podczas pracy

- Przebywanie osób trzecich w obszarze, w którym przetwarzane są dane jest dopuszczalne za zgodą ADO lub w obecności osoby upoważnionej.
- Osoba przetwarzająca dane po zakończeniu pracy porządkuje swoje stanowisko odpowiednio zabezpieczając dostęp do dokumentów i nośników z danymi.
- Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki lub za pośrednictwem firmy zajmującej się niszczeniem dokumentów. Każdy dokument zawierający dane, a nieużyteczny niszczy się niezwłocznie.
- Podczas korzystania z urządzeń wielofunkcyjnych (drukarek, kserokopiarek, etc.) należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu.

Polityka haseł

- Każdy użytkownik systemu informatycznego posiada unikalny identyfikator i ustalone przez siebie hasło autoryzujące jego osobę w systemie informatycznym.
- Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.
- Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła (prócz pierwszego hasła do systemu nadawanego przez Office IT/Helpdesk) i jego przechowywanie.
- Każdy użytkownik posiadający dostęp do systemów informatycznych LP jest obowiązany do:
  - zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystanych do pracy w systemie informatycznym;
  - cyklicznej zmiany haseł w określonych odstępach czasu;
  - niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia;
  - niezwłocznej zmiany hasła tymczasowego, przekazanego przez Office IT/Helpdesk;
  - poinformowania Office IT/Helpdesk oraz IOD o podejrzeniu lub rzeczywistym ujawnieniu hasła;
- Hasła zachowują swoją poufność również po ustaniu ich użyteczności.
- Zabronione jest:
  - zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób;
  - stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.;
  - stosowania haseł posiadających w swojej strukturze części loginu, nazwy firmy lub jej skrótów (np. Payback123, Payback2016, etc.).
  - używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach;
  - udostępnianie haseł innym użytkownikom.

Zasady korzystania z sieci publicznej (Internet)

- Aktywności użytkownika w sieci ze względów bezpieczeństwa są rejestrowane.

- Zdalne korzystanie z systemów informatycznych LP poprzez sieć publiczną jest możliwe jedynie po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji (VPN).
- Ze względów bezpieczeństwa protokoły wymiany danych (FTP) zostały wyłączone.
- Zabronione jest:
  - przeglądanie, przechowywanie i udostępnianie treści uznanych za pornograficzne, rasistowskie, traktujące o przemocy, przestępstwach, jak również do protokołów umożliwiających wymianę plików w sieciach z naruszeniem przepisów prawa;
  - odwiedzanie witryn WWW o podejrzanej/wątpliwej reputacji ze względu na znaczne ryzyko zainfekowania wirusem;
  - samodzielne ściąganie i instalowanie oprogramowania. Każda taka potrzeba powinna być konsultowana z Office IT/Helpdesk.
- Korzystanie z publicznych usług cloud'owych jest dozwolone jedynie po akceptacji Office IT/Helpdesk.

Zasady korzystania ze służbowej poczty elektronicznej

- Użytkownikowi zostaje nadany dedykowany adres skrzynki poczty elektronicznej działający w domenie LP.
- Nadany użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub umownych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych LP podlega rejestrowaniu i może być monitorowana. Informacje przesyłane za pośrednictwem sieci LP (w tym do i z Internetu) nie stanowią własności prywatnej użytkownika.
- Zabronione jest:
  - korzystanie z systemu poczty elektronicznej dla celów prywatnych;
  - wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu);
  - wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi LP;
  - odbieranie przesyłek z nieznanych źródeł;
  - otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.;
  - przesyłanie pocztą elektroniczną plików wykonywalnych typu: bat, com, exe, plików multimedialnych;
  - ukrywanie lub dokonywanie zmian tożsamości nadawcy;
  - czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika;
  - odpowiadanie na niezamówione wiadomości reklamowe oraz na inne formy wymiany danych określanych spamem; w przypadku otrzymania takiej wiadomości należy przesłać ją do Office IT/Helpdesk;
  - posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych;
  - wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb LP lub do poszukiwania dodatkowego zatrudnienia.

Zasady postępowania ze sprzętem komputerowym

- Do sprzętu komputerowego zalicza się między innymi:
  - komputery (stacjonarne i przenośne);
  - telefony komórkowe;
  - nośniki elektroniczne;
  - klucze VPN;
  - osprzęt dostarczony razem z wyżej wymienionym sprzętem lub zakupiony oddzielnie, a w szczególności: zasilacze, torby, klawiatury, myszki komputerowe, etc.
- Zabronione jest:
  - przechowywanie danych firmowych na urządzeniach prywatnych;
  - przechowywanie danych prywatnych na serwerach sieciowych LP;

- Wszelkie zmiany w oprogramowaniu sprzętu komputerowego mogą być wykonywane tylko za pośrednictwem Office IT/Helpdesk.
- Każdy użytkownik sprzętu komputerowego oraz elektronicznych kart dostępu ponosi całkowitą odpowiedzialność za powierzony do użytkowania sprzęt oraz jest zobowiązany do stosowania się do poniższych zasad:
  - Zabrania się pozostawiania powierzonego sprzętu bez opieki w miejscach publicznych;
  - Zabrania się udostępniania powierzonego sprzętu osobom trzecim;
  - Komputery przenośne należy przewozić jako bagaż podręczny;
  - Użytkownik wykonując czynności zawodowe w domu powinien zadbać o należyte zabezpieczenie powierzonego sprzętu oraz dostępu do informacji przed nieautoryzowanym dostępem osób trzecich;
  - Problemy wynikające z nieprawidłowego funkcjonowania sprzętu komputerowego należy zgłaszać Office IT/Helpdesk.
  - W przypadku utraty powierzonego sprzętu należy ten fakt bezzwłocznie zgłosić do IOD oraz Incident Management Team Zgłoszenie należy przesłać niezwłocznie na adres mojedane@payback.net lub LPP_Incident_Management_Team@payback.net W zgłoszeniu należy opisać charakter zdarzenia, w tym okoliczności w jakich do zdarzenia doszło oraz w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane mogą być takim zdarzeniem dotknięte. Incident Management Team zajmie się zgłoszeniem oceniając wagę naruszenia, wprowadzając środki zaradcze oraz podejmując decyzję o ewentualnych zgłoszeniu incydentu do Prezesa Urzędu Ochrony Danych Osobowych.

Ustalenia końcowe

Przedstawione zasady wchodzą w życie **z dniem 26.03.2019.**

Zarząd Loyalty Partner Polska sp. z o.o.

Marcin Pilarski
Członek Zarządu
Loyalty Partner Polska Sp. z o.o.