Środki techniczne i organizacyjne Worldline Financial Services (Europe) S.A.

(EU PL)

1 Cel niniejszego dokumentu

Niniejszy dokument zawiera spis środków technicznych i organizacyjnych stosowanych jako standardowe. Faktycznie powzięte środki zależą od Usługi i lokalizacji przetwarzania z uwagi na to, że nie wszystkie środki będą miały zastosowanie w przypadku każdej Usługi i lokalizacji. Worldline w ramach wszystkich Usług i lokalizacji gwarantuje odpowiednie środki techniczne i operacyjne wymienione w poniższym spisie, które zostały określone w wyniku Oceny skutków w zakresie ochrony danych. Środki te zostały opracowane w celu:

- zapewnienia ochrony i poufności Danych osobowych;
- ochrony bezpieczeństwa i integralności Danych osobowych przed oczekiwanymi zagrożeniami lub niebezpieczeństwami;
- ochrony Danych osobowych przed nieuprawnionym przetwarzaniem w dowolnej formie, ich utratą, wykorzystaniem, ujawnieniem lub pozyskaniem bądź uzyskaniem do nich dostępu.

Na stronie zawarto również spis podwykonawców świadczących usługi w imieniu Worldline. Worldline zapewnia udzielenie przez każdego z naszych podwykonawców odpowiednich gwarancji w ramach ochrony danych osobowych, które są przez nich przetwarzane w naszym imieniu, w formie uczestnictwa w czynnościach kontrolnych wobec podwykonawców: przetwarzanie danych nie powinno być zlecane w przypadku danych w rozumieniu rozporządzenia RODO, art. 28, bez stosownych instrukcji ze strony mocodawcy, np. wyraźnego wskazania w umowie, sformalizowanego sposobu zarządzania podwykonawstwem oraz rygorystycznej selekcji podmiotów przetwarzających (certyfikacja ISO, ISMS), wcześniejszej demonstracji kompetencji, dalszego monitorowania wyników.
Worldline zobowiązuje się stale monitorować skuteczność zabezpieczeń dotyczących informacji oraz raz w roku zlecać wykonanie audytu zgodności Stronie trzeciej w celu zapewnienia wdrożenia środków i stosowanych czynności kontrolnych.

2 Środki techniczne i organizacyjne

A Ludzie, świadomość i HR:

- wszelka rekrutacja odbywa się według procesu kontroli zgodnego z zasadami polityki Worldline dotyczącej sprawdzania przeszłości;
- każdy pracownik, niezależnie od umowy, podpisuje też umowę o zachowaniu poufności;
- każdy pracownik ma obowiązek raz w roku odbyć szkolenie z zakresu Kodeksu etyki (w tym zdania testu), które odbywa się na dedykowanej platformie do e-nauczania;
- polityka dotycząca Dopuszczalnego użytkowania Group IT zostaje udostępniona wszystkim pracownikom;
- podpisana przez Zarząd deklaracja polityki bezpieczeństwa zostaje udostępniona wszystkim pracownikom;
- kadra Worldline zobowiązana jest raz w roku odbyć szkolenia (zakończone testem) z zakresu polityki Ochrony danych Worldline oraz Ochrony i bezpieczeństwa informacji;
- regularne szkolenia uświadamiające w zakresie RODO dla wszystkich pracowników (jako dodatek do szkoleń w zakresie polityki Ochrony danych Worldline oraz Ochrony i bezpieczeństwa informacji);
- dostęp do systemów udzielany jest w zakresie niezbędnym do wypełniania obowiązków, z uwzględnieniem ich podziału;
- regularnie przeprowadzane są wewnętrzne audyty bezpieczeństwa w celu weryfikacji stosowania właściwych praktyk.

B Bezpieczeństwo fizyczne i dokumentacja papierowa:

Zgodność z polityką ochrony fizycznej i środowiskowej Group Worldline:

- wdrożone systemy kontroli dostępu i zarządzania odwiedzinami każdego odwiedzającego/gościa;
- kontrola dostępu (ochrona przed nieupoważnionym dostępem do infrastruktury przetwarzania lub przechowywania danych): w szczególności z wykorzystaniem kart magnetycznych lub inteligentnych, elektrycznych mechanizmów otwierania drzwi, portierów, pracowników ochrony, systemów alarmowych, systemów wideo;
- przeglądy dostępu przeprowadzane w ustalonej częstotliwości;
- wdrożone procedury zachowywania porządku na biurku, czyszczenia ekranu i drukowania w trybie „follow me";
- informacje, w tym dokumenty w formie papierowej, obsługiwane przez importera danych są niejawne, oznaczone, chronione i podlegają przepływowi zgodnie z polityką utajniania informacji Worldline;
- komputery stacjonarne nie są wynoszone z siedziby z wyjątkiem uzyskania wcześniej szczególnego upoważnienia;
- monitoring CCTV w celu ochrony obszarów zastrzeżonych;
- wdrożone alarmy i systemy przeciwpożarowe w celu zapewnienia bezpieczeństwa pracowników;
- w określonej częstotliwości przeprowadzane są ćwiczenia ewakuacji na wypadek pożaru;

C Ochrona zdalnie połączonych urządzeń użytkowników końcowych

Użytkownicy zdalni pracują na laptopach lub komputerach stacjonarnych podłączonych do zabezpieczonej sieci Worldline, którą w imieniu Worldline Group utrzymuje Global IT. Ponadto wdrożone są następujące środki ochrony:

- szyfrowanie dysków twardych w laptopach firmowych;
- weryfikacja dwuetapowa (PKI/rozwiązania alternatywne);
- zarządzanie centralne oraz ochrona antywirusowa;
- zarządzanie oprogramowaniem i monitorowanie w celu kontroli nieupoważnionej instalacji oprogramowania;
- kontrola identyfikatorów i haseł dostępowych do informacji;
- okresowe przeglądy dostępu;
- automatyczne skanowanie e-maili programem antywirusowym i antyspamowym.

D Ochrona dostępu zdalnego

Dostęp zdalny do krytycznych systemów docelowych Worldline z reguły wymaga weryfikacji dwuetapowej. Jeśli źródłem połączenia zdalnego jest system będący pod kontrolą Worldline, wdrożona jest metoda weryfikacji oparta o certyfikat danego urządzenia.
Połączenia wykonywane na jakiekolwiek inne sposoby muszą być najpierw zatwierdzone przez dział bezpieczeństwa.

E Ogólne środki ochrony to m.in.:

- przechowywanie danych w Centrach danych na terenie UE i Szwajcarii, a w przypadku laptopów dane są szyfrowane na urządzeniu lokalnym;
- przerywanie połączeń dostępowych w strefach zdemilitaryzowanych;
- cała łączność do obszarów chronionych (strefy PCI) jest szyfrowana;
- dostęp do strefy PCI możliwy jest wyłącznie na drodze wzmocnionego uwierzytelnienia za pośrednictwem udostępnionego klienta ochrony;
- na drodze stoją wielowarstwowe firewalle i systemy wykrywania wtargnięć;
- zarządzanie dostępem w myśl zasad Kontroli dostępu w zależności od roli;
- zarządzanie prywatnością, w tym regularne szkolenia pracowników;
- zarządzanie reakcjami na zdarzenia;
- ustawienia domyślne zapewniające prywatność.

F Kontrola dostępu do Danych osobowych

Pracownicy pracujący z danymi osobowymi mają dostęp jedynie do tych danych, które są im niezbędne do wykonywania swoich obowiązków. Uprawnienia dostępu udzielane jest w oparciu o zasadę ograniczonej wiedzy i ograniczonego dostępu oraz zależą od roli pracownika lub nazwiska. Istnieją dzienniki dostępowe oraz przydzielone są obowiązki związane z kontrolą dostępu.

Stosowane są następujące środki:

- pracownicy mają obowiązek przestrzegania odpowiednich polityk Worldline oraz lokalnych polityk dotyczących ochrony danych;
- instrukcje robocze dotyczące obchodzenia się z danymi prywatnymi;
- elektroniczny system kontroli dostępu (ochrona przed nieupoważnionym wykorzystaniem systemów przetwarzania lub przechowywania danych), w szczególności z wykorzystaniem haseł (w tym odpowiedniej polityki), automatycznych mechanizmów zamykających, weryfikacji dwuetapowej, szyfrowania nośników danych;
- wewnętrzny system kontroli dostępu (zapobiegający nieupoważnionemu odczytywaniu, kopiowaniu, modyfikowaniu lub usuwaniu danych w sieci Worldline), tj. wykorzystanie profilów autoryzacji standardowej w oparciu o zasadę ograniczonego dostępu, standardowy proces przyznawania praw użytkownika, logowanie w celu uzyskania dostępu, okresowe przeglądy przyznanych praw, zwłaszcza jeśli chodzi o konta administratorów;
- proces kontrolowanego niszczenia nośników danych;
- wdrożone procedury Kontroli zgodności z procedurami oraz instrukcjami roboczymi;

110.0788.05 EU_PL/04.2022

G Ochrona i poufność danych osobowych

Worldline zapewnia odpowiedni poziom ochrony zdefiniowany na podstawie oceny ryzyka (oraz oceny skutków w zakresie ochrony danych, jeśli jest taka potrzeba), m.in.:

- plan klasyfikacji danych: kategoryzację danych osobowych według stopnia poufności określonego przez wymogi prawne lub w drodze samooceny;
- brak możliwości odczytu, kopiowania, modyfikowania lub usuwania danych bez upoważnienia w trakcie ich transmisji lub przekazywania w formie elektronicznej, w szczególności z wykorzystaniem szyfrowania i prywatnych sieci wirtualnych (VPN);
- możliwość utrzymania utajnienia, integralności, dostępności oraz trwałości systemów i usług przetwarzania danych w sposób ciągły;
- ochrona przed przypadkowym lub umyślnym zniszczeniem danych bądź ich utratą, jak np. strategia tworzenia kopii zapasowych (online/offline, w firmie/poza firmą), nieprzerwane zasilanie energią elektryczną (zasilacz UPS, zespół agregatów wysokoprężnych), program antywirusowy, firewall, kanały alarmowe i plany awaryjne, kontrole zabezpieczeń infrastruktury i aplikacji, wielopoziomowy plan ochrony z oddelegowaniem przechowywania kopii zapasowych do centrów danych kopii zapasowych, standardowe procesy na wypadek zmian/zwolnień pracowników;
- możliwość przywrócenia dostępności i dostępu do Danych osobowych w krótkim czasie na wypadek problemów technicznych lub wypadku;
- proces regularnego testowania, analizy oraz oceny skuteczności środków technicznych i organizacyjnych w celu zapewnienia ochrony przetwarzanych danych (audyt wewnętrzny, PCI-DSS, ISO 27001, krajowe organy nadzorcze);
- rejestry procesów zgodnie z wymogami RODO;
- możliwość wykorzystania systemów dzienników dostępu w celu wykrycia nieupoważnionych prób uzyskania dostępu;
- w przypadku klienta głównego Dane i metadane (w tym kopie zapasowe, archiwa, pliki dziennika itp.) będą przechowywane tylko tak długo, jak będzie to konieczne w związku celem ich gromadzenia, chyba że istnieje prawny lub umowny obowiązek zachowania danych przez dłuższy czas.

H Kontrola organizacji

Jednostka przetwarzania danych zachowuje integralność organizacyjną w sposób zgodny z wymogami odpowiednich przepisów prawnych oraz wymagań Administratora danych w zakresie ochrony danych. Jest to osiągnięte za pomocą:

wewnętrznych polityk i procedur dotyczących przetwarzania danych, wytycznych, instrukcji roboczych, opisów procesów oraz przepisów dotyczących programowania, testowania i publikacji w zakresie, w jakim działania te dotyczą Danych osobowych przesyłanych przez Administratora;

wdrożenia ramowego planu kontroli nad Ochroną danych, który raz do roku zostanie poddany audytowi w kierunku zgodności;

posiadania planu awaryjnego ze sprecyzowanymi procedurami i przydziałem obowiązków (zapasowy plan awaryjny).