Warszawa, 05.08.2025 r.

AKT O USŁUGACH DANYCH – INFORMACJE O USŁUGACH

Informacje dotyczące usługi przetwarzania danych: IP GATE

1. Informacje o istniejących procedurach zmiany dostawcy i przeniesienia usługi przetwarzania danych, w tym informacje o dostępnych metodach i formatach zmiany dostawcy i przeniesienia oraz o limitach i ograniczeniach technicznych znanych dostawcy usług przetwarzania danych.

   Klient ma prawo do zmiany dostawcy usługi IP Gate na innego dostawcę usług przetwarzania danych tego samego typu (oferujących hosting poczty elektronicznej i stron WWW z możliwością zarządzania domenami, kontami pocztowymi oraz FTP) lub do przeniesienia danych i zasobów cyfrowych do własnej infrastruktury. T-Mobile nie stawia żadnych limitów i ograniczeń technicznych w tym zakresie.

2. Informacje o strukturach danych i formatach danych oraz o stosownych normach i otwartych specyfikacjach w zakresie interoperacyjności, w których dostępne są dane eksportowalne.

   W trakcie korzystania z usługi zbierane są następujące dane:

   a. Pliki stron WWW i pliki serwera FTP, które Klient może pobrać samodzielnie na swoje zasoby, za pomocą posiadanych przez siebie narzędzi typu klient FTP (np. Total Commander lub WinSCP). Klient może również zawnioskować do T-Mobile o zebranie wszystkich plików do folderu zapisanego w formacie .ZIP.
   b. Bazy danych MySQL, które Klient może pobrać samodzielnie na swoje zasoby za pomocą panelu administracyjnego WebAdmin (https://webadmin.ipgate.t-mobile.pl) stanowiącego część panelu administracyjnego Usługi. Są to pliki płaskie z rozszerzeniem .sql, zawierające zrzuty baz danych wraz z tabelami i rekordami.
   c. Pliki ze strefami DNS. Pliki ze strefą DNS Klienta możliwe są do przekazania w formacie .txt.
   d. Zapisane wiadomości e-mail ze skrzynki pocztowej, stanowiące pliki płaskie zawierające nagłówki STMP wraz z treścią wiadomości w postaci zaszyfrowanej lub niezaszyfrowanej, w zależności od ustawień skrzynki pocztowej, administrowanej przez Klienta.

3. Jurysdykcja, której podlega infrastruktura ICT używana do przetwarzania danych w ramach ich poszczególnych usług.

   Usługa podlega jurysdykcji Rzeczpospolitej Polskiej.

4. Środki techniczne, organizacyjne i umowne przyjęte w celu zapobieżenia międzynarodowemu dostępowi do danych nieosobowych przechowywanych na terenie Unii lub ich przekazania administracji rządowej, w przypadku, gdy taki dostęp lub takie przekazanie skutkowałoby naruszeniem prawa Unii lub prawa krajowego danego państwa członkowskiego.

   Dla usługi IP Gate spełnione są wymagania normy Systemu Zarządzania Bezpieczeństwem Informacji ISO/IEC 27001:2022 z zastosowaniem zabezpieczeń przewidzianych w ISO/IEC 27017:2015 i ISO/IEC 27018:2019, co jest potwierdzone certyfikatem dostępnym na stronie: https://biznes.t-mobile.pl/pl/obsluga-klienta/dokumenty/normy-iso.

5. Informacje o usługach przetwarzania danych, które wiążą się z wysoce złożoną lub kosztowną zmianą dostawcy lub z niemożnością zmiany dostawcy bez znacznej ingerencji w dane, aktywa cyfrowe lub architekturę usługi.

   Nie dotyczy usługi IP Gate.

Informacje dotyczące usługi przetwarzania danych: BACKUP

1. Informacje o istniejących procedurach zmiany dostawcy i przeniesienia usługi przetwarzania danych, w tym informacje o dostępnych metodach i formatach zmiany dostawcy i przeniesienia oraz o limitach i ograniczeniach technicznych znanych dostawcy usług przetwarzania danych.

   Zgodnie z art. 26 lit. a) oraz art. 30 ust. 1 i 2 rozporządzenia (UE) 2023/2854 („Data Act”), usługa Backup umożliwia zmianę dostawcy oraz przeniesienie danych w formatach nadających się do ponownego użycia. Dane mogą być eksportowane przez użytkownika wyłącznie na jego wniosek, z wykorzystaniem bezpiecznych kanałów transmisji. Znane ograniczenia techniczne obejmują konieczność czasowego wstrzymania maszyn wirtualnych w celu wykonania poprawnej migracji do nowego dostawcy. Dostawca zapewnia wsparcie techniczne oraz dokumentację niezbędną do realizacji procesu migracji.

2. Informacje o strukturach danych i formatach danych oraz o stosownych normach i otwartych specyfikacjach w zakresie interoperacyjności, w których dostępne są dane eksportowalne.

Format danych eksportowanych

Typ backup	Typ pliku / Rozszerzenie	Opis techniczny
NetBackup	.nbf, .nbk, .tar, .img	Pliki backupu pełnego i przyrostowego, często w formacie tar lub obrazów dysków.
Avamar	.avamar, .vmdk, .vhdx, .tar	Pliki backupu danych, często deduplikowane; obsługuje formaty dysków wirtualnych dla VMware i Hyper-V
Commvault	.cvbak, .xml	Pliki backupu w formacie natywnym

3. Jurysdykcja, której podlega infrastruktura ICT używana do przetwarzania danych w ramach ich poszczególnych usług.

   Przechowywanie danych wyłącznie w centrach danych zlokalizowanych na terytorium UE (DC Piaseczno, Szlachecka, Wrocław, Kraków), posiadających certyfikaty ISO/IEC 27001:2022, ISO 22301:2019, ISO 9001, ISO 14001 oraz ISO 45001 1

4. Środki techniczne, organizacyjne i umowne przyjęte w celu zapobieżenia międzynarodowemu dostępowi do danych nieosobowych przechowywanych na terenie Unii lub ich przekazania administracji rządowej, w przypadku, gdy taki dostęp lub takie przekazanie skutkowałoby naruszeniem prawa Unii lub prawa krajowego danego państwa członkowskiego.

   Zgodnie z art. 5 ust. 1 lit. a) Data Act, dostawca usługi Backup as a Service wdrożył środki techniczne mające na celu uniemożliwienie nieuprawnionego dostępu do danych nieosobowych przez podmioty trzecie spoza Unii Europejskiej, w tym:

   - przechowywanie danych wyłącznie w centrach danych zlokalizowanych na terytorium UE (Piaseczno i Kraków), posiadających certyfikaty ISO/IEC 27001:2022, ISO 22301:2019, ISO 9001, ISO 14001 oraz ISO 45001 1;
   - zastosowanie mechanizmów kontroli dostępu, szyfrowania danych oraz monitorowania integralności danych;
   - zapewnienie możliwości wyboru lokalizacji przechowywania danych przez użytkownika końcowego (do wyboru kilka lokalizacji)
   - procedury reagowania na incydenty bezpieczeństwa i naruszenia ochrony danych;
   - polityki zarządzania dostępem oraz retencją danych;
   - dokumentację wewnętrzną potwierdzającą zgodność z przepisami UE w zakresie ochrony danych nieosobowych. (Dokument P-LD-00-01 opisuje procedurę bezpieczeństwa informacji i ochrony danych w T-Mobile Polska. Zawiera zasady klasyfikacji informacji (np. „Ogólnodostępne", „Wewnętrzne T-Mobile", „Poufne T-Mobile", „Ściśle Poufne T-Mobile") oraz wymagania dotyczące ich zabezpieczenia zgodnie z regulacjami prawnymi i interesem spółki)

5. Informacje o usługach przetwarzania danych, które wiążą się z wysoce złożoną lub kosztowną zmianą dostawcy lub z niemożnością zmiany dostawcy bez znacznej ingerencji w dane, aktywa cyfrowe lub architekturę usługi.

   Zmiana dostawcy usługi Business Backup może być złożona i kosztowna ze względu na specyfikę technologiczną środowiska backupowego, w tym zamknięte formaty danych, szyfrowanie i zależność od metadanych. Wymaga to czasowego wstrzymania usług oraz dostosowania infrastruktury po stronie nowego dostawcy z zastosowaniem tego samego oprogramowania. Dane są udostępniane w formatach interoperacyjnych, ale ich migracja może wiązać się z ryzykiem utraty integralności. T-Mobile Polska umożliwia i rekomenduje tzw. model dual access, w którym klient tworzy nowe kopie u nowego dostawcy, a dotychczasowy zapewnia dostęp do danych historycznych przez okres przejściowy. Zgodnie z Data Act, dostawca ma obowiązek usunięcia przeszkód technicznych i zapewnienia wsparcia w procesie zmiany. Klient nie traci prawa do danych i może je tym samym odtworzyć w sposób bezpieczny i zgodny z przepisami.

Informacje dotyczące usługi przetwarzania danych: BUSINESS BACKUP

1. Informacje o istniejących procedurach zmiany dostawcy i przeniesienia usługi przetwarzania danych, w tym informacje o dostępnych metodach i formatach zmiany dostawcy i przeniesienia oraz o limitach i ograniczeniach technicznych znanych dostawcy usług przetwarzania danych.

   Zgodnie z art. 26 lit. a) oraz art. 30 ust. 1 i 2 rozporządzenia (UE) 2023/2854 („Data Act"), usługa Business Backup umożliwia zmianę dostawcy oraz przeniesienie danych w formatach nadających się do ponownego użycia. Dane mogą być eksportowane przez użytkownika wyłącznie na jego wniosek, z wykorzystaniem bezpiecznych kanałów transmisji. Znane ograniczenia techniczne obejmują konieczność czasowego wstrzymania maszyn wirtualnych w celu wykonania poprawnej migracji do nowego dostawcy. Dostawca zapewnia wsparcie techniczne oraz dokumentację niezbędną do realizacji procesu migracji.

2. Informacje o strukturach danych i formatach danych oraz o stosownych normach i otwartych specyfikacjach w zakresie interoperacyjności, w których dostępne są dane eksportowalne.

   Format danych eksportowanych

Typ danych	Format pliku	Opis techniczny
Pełny backup	.vbk	Standalone Full Backup – zawiera pełny obraz maszyny lub systemu
Backup przyrostowy	.vib	Incremental Backup – zawiera zmiany względem poprzedniego punktu
Backup syntetyczny	.vrb	Reverse Incremental – alternatywna metoda backupu przyrostowego
Eksport dysków VM	.vmdk, .vhdx	Format dysków wirtualnych dla VMware i Hyper-

3. Jurysdykcja, której podlega infrastruktura ICT używana do przetwarzania danych w ramach ich poszczególnych usług.

   Przechowywanie danych wyłącznie w centrach danych zlokalizowanych na terytorium UE (DC Piaseczno, Szlachecka, Wrocław, Kraków), posiadających certyfikaty ISO/IEC 27001:2022, ISO 22301:2019, ISO 9001, ISO 14001 oraz ISO 45001 1

4. Środki techniczne, organizacyjne i umowne przyjęte w celu zapobieżenia międzynarodowemu dostępowi do danych nieosobowych przechowywanych na terenie Unii lub ich przekazania administracji rządowej, w przypadku, gdy taki dostęp lub takie przekazanie skutkowałoby naruszeniem prawa Unii lub prawa krajowego danego państwa członkowskiego.

   Data Act, dostawca usługi Business Backup wdrożył środki techniczne mające na celu uniemożliwienie nieuprawnionego dostępu do danych nieosobowych przez podmioty trzecie spoza Unii Europejskiej, w tym:

   - przechowywanie danych wyłącznie w centrach danych zlokalizowanych na terytorium UE (Piaseczno i Kraków), posiadających certyfikaty ISO/IEC 27001:2022, ISO 22301:2019, ISO 9001, ISO 14001 oraz ISO 45001 1;
   - zastosowanie mechanizmów kontroli dostępu, szyfrowania danych oraz monitorowania integralności danych;
   - zapewnienie możliwości wyboru lokalizacji przechowywania danych przez użytkownika końcowego (do wyboru kilka lokalizacji)
   - procedury reagowania na incydenty bezpieczeństwa i naruszenia ochrony danych;
   - polityki zarządzania dostępem oraz retencją danych;
   - dokumentację wewnętrzną potwierdzającą zgodność z przepisami UE w zakresie ochrony danych nieosobowych. (Dokument P-LD-00-01 opisuje procedurę bezpieczeństwa informacji i ochrony danych w T-Mobile Polska. Zawiera zasady klasyfikacji informacji (np. „Ogólnodostępne", „Wewnętrzne T-Mobile", „Poufne T-Mobile", „Ściśle Poufne T-Mobile") oraz wymagania dotyczące ich zabezpieczenia zgodnie z regulacjami prawnymi i interesem spółki)

5. Informacje o usługach przetwarzania danych, które wiążą się z wysoce złożoną lub kosztowną zmianą dostawcy lub z niemożnością zmiany dostawcy bez znacznej ingerencji w dane, aktywa cyfrowe lub architekturę usługi.

   Usługa Business Backup jest usługą przetwarzania danych w rozumieniu Data Act, a proces zmiany dostawcy podlega zasadom interoperacyjności określonym w § 20 Umowy. Klient ma prawo przenieść dane eksportowalne i aktywa cyfrowe w formatach technicznych wskazanych w Tabeli nr 5 (.vbk, .vib, .vrb, .vmdk, .vhdx), z wykorzystaniem narzędzi udostępnionych przez producenta oprogramowania (Veeam). W trakcie Okresu Przejściowego Klient samodzielnie pobiera dane, a T-Mobile zapewnia wsparcie techniczne oraz bezpieczeństwo danych. Dane wyłączone z eksportu zostały określone w Tabeli nr 6 i obejmują m.in. konfiguracje środowiska backupowego oraz informacje poufne T-Mobile Polska. W przypadku wystąpienia ograniczeń technicznych T-Mobile Polska umożliwia i rekomenduje tzw. model dual access, w którym klient tworzy nowe kopie u nowego dostawcy, a dotychczasowy zapewnia dostęp do danych historycznych przez okres przejściowy. Zgodnie z Data Act, dostawca ma obowiązek usunięcia przeszkód technicznych i zapewnienia wsparcia w procesie zmiany. Klient nie traci prawa do danych i może je tym samym odtworzyć w sposób bezpieczny i zgodny z przepisami.

Informacje dotyczące usługi przetwarzania danych: SERWER DEDYKOWANY W OPCJI PRIVATE CLOUD

1. Informacje o istniejących procedurach zmiany dostawcy i przeniesienia usługi przetwarzania danych, w tym informacje o dostępnych metodach i formatach zmiany dostawcy i przeniesienia oraz o limitach i ograniczeniach technicznych znanych dostawcy usług przetwarzania danych.

   Zgodnie z art. 26 lit. a) oraz art. 30 ust. 1 i 2 rozporządzenia (UE) 2023/2854 („Data Act"), usługa Serwer Dedykowany w opcji Private Cloud umożliwia zmianę dostawcy oraz przeniesienie danych w formatach nadających się do ponownego użycia. Dane mogą być eksportowane przez użytkownika wyłącznie na jego wniosek, z wykorzystaniem bezpiecznych kanałów transmisji. Znane ograniczenia techniczne obejmują konieczność czasowego wstrzymania maszyn wirtualnych w celu wykonania poprawnej migracji do nowego dostawcy. Dostawca zapewnia wsparcie techniczne oraz dokumentację niezbędną do realizacji procesu migracji.

2. Informacje o strukturach danych i formatach danych oraz o stosownych normach i otwartych specyfikacjach w zakresie interoperacyjności, w których dostępne są dane eksportowalne

   Format danych eksportowanych

   VMware

Typ danych	Format	Opis
Obraz maszyny wirtualnej	.ovf + .vmdk	OVF (Open Virtualization Format) zawiera plik konfiguracyjny maszyny, a VMDK to dysk wirtualny
Eksport z RVTools	.xlsx	Metadane o konfiguracji maszyn (CPU, RAM, sieć, storage) w formacie Excel

   Microsoft Hyper - V

Typ danych	Format	Opis
Obraz maszyny wirtualnej	.vhdx	Dysk wirtualny maszyny Hyper-V
Konfiguracja maszyny	.xml	Plik konfiguracyjny maszyny (eksportowany z Hyper-V Manager lub PowerShell)
Eksport z RVTools (jeśli środowisko heterogeniczne)	.xlsx	Metadane w formacie Excel (jeśli używane narzędzie wspiera Hyper-V)

3. Jurysdykcja, której podlega infrastruktura ICT używana do przetwarzania danych w ramach ich poszczególnych usług

   Przechowywanie danych wyłącznie w centrach danych zlokalizowanych na terytorium UE (DC Piaseczno, Szlachecka, Wrocław, Kraków), posiadających certyfikaty ISO/IEC 27001:2022, ISO 22301:2019, ISO 9001, ISO 14001 oraz ISO 45001 1;

4. Środki techniczne, organizacyjne i umowne przyjęte w celu zapobieżenia międzynarodowemu dostępowi do danych nieosobowych przechowywanych na terenie Unii lub ich przekazania administracji rządowej, w przypadku, gdy taki dostęp lub takie przekazanie skutkowałyby naruszeniem prawa Unii lub prawa krajowego danego państwa członkowskiego.

   Zgodnie z art. 5 ust. 1 lit. a) Data Act, dostawca usługi Private Cloud wdrożył środki techniczne mające na celu uniemożliwienie nieuprawnionego dostępu do danych nieosobowych przez podmioty trzecie spoza Unii Europejskiej, w tym:

   - przechowywanie danych wyłącznie w centrach danych zlokalizowanych na terytorium UE (Piaseczno i Kraków), posiadających certyfikaty ISO/IEC 27001:2022, ISO 22301:2019, ISO 9001, ISO 14001 oraz ISO 45001 1;
   - zastosowanie mechanizmów kontroli dostępu, szyfrowania danych oraz monitorowania integralności danych;
   - zapewnienie możliwości wyboru lokalizacji przechowywania danych przez użytkownika końcowego (do wyboru kilka lokalizacji)
   - procedury reagowania na incydenty bezpieczeństwa i naruszenia ochrony danych;
   - polityki zarządzania dostępem oraz retencją danych;
   - dokumentację wewnętrzną potwierdzającą zgodność z przepisami UE w zakresie ochrony danych nieosobowych. (Dokument P-LD-00-01 opisuje procedurę bezpieczeństwa informacji i ochrony danych w T-Mobile Polska. Zawiera zasady klasyfikacji informacji (np. „Ogólnodostępne", „Wewnętrzne T-Mobile", „Poufne T-Mobile", „Ściśle Poufne T-Mobile") oraz wymagania dotyczące ich zabezpieczenia zgodnie z regulacjami prawnymi i interesem spółki)

5. Informacje o usługach przetwarzania danych, które wiążą się z wysoce złożoną lub kosztowną zmianą dostawcy lub z niemożnością zmiany dostawcy bez znacznej ingerencji w dane, aktywa cyfrowe lub architekturę usługi.

Obszar usługi	Potencjalna trudność zmiany dostawcy	Uzasadnienie
Oprogramowanie wirtualizacyjne (np. VMware)	Wysoka	Środowisko oparte na licencjonowanym oprogramowaniu producenta. Migracja do innego środowiska (np. Hyper-V, KVM) może wymagać konwersji formatów, zmiany architektury i ponownej konfiguracji maszyn wirtualnych.
Formaty danych maszyn wirtualnych	Średnia	Dane są udostępniane w formatach zgodnych z aktualną platformą (OVF + VMDK lub VHDX). Zmiana dostawcy może wymagać konwersji do innych formatów, co wiąże się z dodatkowymi nakładami technicznymi.
Licencje systemów operacyjnych i baz danych	Wysoka	Licencje mogą być przypisane do infrastruktury TMPL i nieprzenoszalne. Klient może być zobowiązany do zakupu nowych licencji u nowego dostawcy.
Brak automatycznych	Średnia	TMPL nie zapewnia automatycznych narzędzi do migracji do innych środowisk. Migracja odbywa się na żądanie klienta, ręcznie.

Obszar usługi	Potencjalna trudność zmiany dostawcy	Uzasadnienie
narzędzi migracyjnych		

Informacje dotyczące usługi przetwarzania danych: METROCLUSTER

1. Informacje o istniejących procedurach zmiany dostawcy i przeniesienia usługi przetwarzania danych, w tym informacje o dostępnych metodach i formatach zmiany dostawcy i przeniesienia oraz o limitach i ograniczeniach technicznych znanych dostawcy usług przetwarzania danych.

   Klient ma prawo do zmiany dostawcy usługi Wirtualne Centrum Danych na innego dostawcę usług przetwarzania danych tego samego typu (oferujących usługi w modelu Infrastrukturę as a Service , oparte o wirtualizację firmy VMware/Broadcom) lub do przeniesienia danych i zasobów cyfrowych do własnej infrastruktury. T-Mobile nie stawia żadnych limitów i ograniczeń technicznych w tym zakresie.

2. Informacje o strukturach danych i formatach danych oraz o stosownych normach i otwartych specyfikacjach w zakresie interoperacyjności, w których dostępne są dane eksportowalne

   W trakcie korzystania z usługi zbierane są następujące dane:

   e. Obrazy maszyn wirtualnych (wirtualnych serwerów) możliwe do pobrania bezpośrednio z panelu administracyjnego usługi, jako wirtualną aplikację (ang. Virtual Application, vApp), lub w formacie OVA z serwera SFTP udostępnionego na wniosek Klienta przez T-Mobile.
   f. Kopie zapasowe (tzw. backupy) maszyn wirtualnych dla Klientów, którzy wykupili w ramach usługi funkcję Backup, możliwe do pobrania z serwera SFTP udostępnionego na wniosek Klienta przez T-Mobile w formatach: .vbk, .vib, .vrb.
   g. Metadane usługi: dane o konfiguracji wirtualnych serwerów, sieciach oraz konfiguracji EdgeGateway, możliwe do pobrania za pomocą Panelu Administracyjnego oraz poprzez API.
   h. Logi operacyjne: dane związane z logowaniem klienta do Usługi oraz korzystaniem z niej, możliwe do pobrania za pomocą Panelu Administracyjnego oraz poprzez API.

3. Jurysdykcja, której podlega infrastruktura ICT używana do przetwarzania danych w ramach ich poszczególnych usług

   Usługa podlega jurysdykcji Rzeczpospolitej Polskiej.

4. Środki techniczne, organizacyjne i umowne przyjęte w celu zapobieżenia międzynarodowemu dostępowi do danych nieosobowych przechowywanych na terenie Unii lub ich przekazania administracji rządowej, w przypadku, gdy taki dostęp lub takie przekazanie skutkowałyby naruszeniem prawa Unii lub prawa krajowego danego państwa członkowskiego.

   Dla usługi IP Gate spełnione są wymagania normy Systemu Zarządzania Bezpieczeństwem Informacji ISO/IEC 27001:2022 z zastosowaniem zabezpieczeń przewidzianych w ISO/IEC 27017:2015 i ISO/IEC 27018:2019, co jest potwierdzone certyfikatem dostępnym na stronie: https://biznes.t-mobile.pl/pl/obsluga-klienta/dokumenty/normy-iso.

5. Informacje o usługach przetwarzania danych, które wiążą się z wysoce złożoną lub kosztowną zmianą dostawcy lub z niemożnością zmiany dostawcy bez znacznej ingerencji w dane, aktywa cyfrowe lub architekturę usługi.

   Nie dotyczy usługi MetroCluster.

Informacje dotyczące usługi przetwarzania danych: WIRTUALNE CENTRUM DANYCH

1. Informacje o istniejących procedurach zmiany dostawcy i przeniesienia usługi przetwarzania danych, w tym informacje o dostępnych metodach i formatach zmiany dostawcy i przeniesienia oraz o limitach i ograniczeniach technicznych znanych dostawcy usług przetwarzania danych.

   Klient ma prawo do zmiany dostawcy usługi Wirtualne Centrum Danych na innego dostawcę usług przetwarzania danych tego samego typu (oferujących usługi w modelu Infrastrukturę as a Service , oparte o wirtualizację firmy VMware/Broadcom) lub do przeniesienia danych i zasobów cyfrowych do własnej infrastruktury. T-Mobile nie stawia żadnych limitów i ograniczeń technicznych w tym zakresie.

2. Informacje o strukturach danych i formatach danych oraz o stosownych normach i otwartych specyfikacjach w zakresie interoperacyjności, w których dostępne są dane eksportowalne

   W trakcie korzystania z usługi zbierane są następujące dane:

   - Obrazy maszyn wirtualnych (wirtualnych serwerów) możliwe do pobrania bezpośrednio z panelu administracyjnego usługi, jako wirtualną aplikację (ang. Virtual Application, vApp), lub w formacie OVA z serwera SFTP udostępnionego na wniosek Klienta przez T-Mobile.
   - Kopie zapasowe (tzw. backupy) maszyn wirtualnych dla Klientów, którzy wykupili w ramach usługi funkcję Backup, możliwe do pobrania z serwera SFTP udostępnionego na wniosek Klienta przez T-Mobile w formatach: .vbk, .vib, .vrb.
   - Metadane usługi: dane o konfiguracji wirtualnych serwerów, sieciach oraz konfiguracji EdgeGateway, możliwe do pobrania za pomocą Panelu Administracyjnego oraz poprzez API.
   - Logi operacyjne: dane związane z logowaniem klienta do Usługi oraz korzystaniem z niej, możliwe do pobrania za pomocą Panelu Administracyjnego oraz poprzez API.
   - Z zakresu danych eksportowalnych wyłączone zostały replikacje zewnętrznego środowiska Klienta zebrane w ramach trwania usługi Wirtualne Centrum Danych z zastosowaniem DRaaS. Zgromadzone w ich ramach dane zostaną usunięte. Aby zachować ciągłość funkcjonalności DRaaS, Klient powinien na swoim zewnętrznym środowisku wskazać dane nowego dostawcy do przechowywania replikacji.

3. Jurysdykcja, której podlega infrastruktura ICT używana do przetwarzania danych w ramach ich poszczególnych usług

   Usługa podlega prawu Rzeczpospolitej Polskiej.

4. Środki techniczne, organizacyjne i umowne przyjęte w celu zapobieżenia międzynarodowemu dostępowi do danych nieosobowych przechowywanych na terenie Unii lub ich przekazania administracji rządowej, w przypadku, gdy taki dostęp lub takie przekazanie skutkowałyby naruszeniem prawa Unii lub prawa krajowego danego państwa członkowskiego.

   Dla usługi Wirtualne Centrum Danych spełnione są wymagania normy Systemu Zarządzania Bezpieczeństwem Informacji ISO/IEC 27001:2022, co jest potwierdzone certyfikatem dostępnym na stronie: https://biznes.t-mobile.pl/pl/obsluga-klienta/dokumenty/normy-iso.

5. Informacje o usługach przetwarzania danych, które wiążą się z wysoce złożoną lub kosztowną zmianą dostawcy lub z niemożnością zmiany dostawcy bez znacznej ingerencji w dane, aktywa cyfrowe lub architekturę usługi.

   Nie dotyczy usługi Wirtualne Centrum Danych.

Informacje dotyczące usługi przetwarzania danych: WIRTUALNE CALL CENTER

1. Informacje o istniejących procedurach zmiany dostawcy i przeniesienia usługi przetwarzania danych, w tym informacje o dostępnych metodach i formatach zmiany dostawcy i przeniesienia oraz o limitach i ograniczeniach technicznych znanych dostawcy usług przetwarzania danych.

   Klient ma prawo do zmiany dostawcy usługi Wirtualnego Call Center na innego dostawcę usług przetwarzania danych tego samego typu (oferującego i dostarczającego w formie licencji na oprogramowanie i aplikacji do obsługi połączeń z wielu różnych kanałów komunikacji) lub do przeniesienia danych i zasobów cyfrowych do własnej infrastruktury. T-Mobile nie stawia żadnych limitów i ograniczeń technicznych w tym zakresie.

2. Informacje o strukturach danych i formatach danych oraz o stosownych normach i otwartych specyfikacjach w zakresie interoperacyjności, w których dostępne są dane eksportowalne

   Zakres danych eksportowanych w ramach usługi WCC obejmuje dane generowane przez użytkowników i system w ramach normalnej eksploatacji. W szczególności:

   - logi połączeń (numer dzwoniącego, numer docelowy, czas, status, źródło kampanii),
   - nagrania rozmów (w formacie MP3 lub WAV),
   - transkrypcje rozmów (TXT, SRT),
   - dane interakcji omnichannel (czaty, e-maile, formularze),
   - konfiguracje kampanii i routingów,
   - dane agentów (ID, aktywności, dostępność, tagowanie rozmów),
   - dane analityczne (metryki KPI, raporty SLA, oceny jakości).
   - dane administratorów (imię i nazwisko, adres e-mail, numer telefonu),
   - dane użytkowników wewnętrznych i ich ustawienia,
   - książki telefoniczne,
   - informacje o kluczu licencyjnym,
   - komunikaty systemowe,
   - szablony provisioningu telefonów i oprogramowanie do nich,
   - może zawierać tymczasowe pliki audio.

   Conpeek:

   Zakres danych dostępnych do eksportu może być konfigurowany przez klienta z wykorzystaniem API lub interfejsu administracyjnego.

   Dane te są dostępne w formatach:

   - CSV / JSON / XML – dane tabelaryczne i zdarzeniowe,
   - ZIP – zbiorcze archiwa eksportowe,
   - MP3/WAV/FLAC/TXT– treści konwersacyjne i nagrania.

   Halo2:

   Wszystkie dane są umieszczane w jednym, skompresowanym pliku .ZIP, który może dodatkowo zostać zabezpieczony hasłem.

   Aplikacja umożliwia eksport do pliku .ZIP, który zawiera:

   - pliki binarne (dla oprogramowania telefonów itp.),
   - .WAV (dla nagrań tymczasowych, komunikatów) oraz
   - .SQL (skrypty migracyjne bazy danych PostgreSQL).

3. Jurysdykcja, której podlega infrastruktura ICT używana do przetwarzania danych w ramach ich poszczególnych usług

   Usługa podlega prawu Rzeczypospolitej Polskiej.

4. Środki techniczne, organizacyjne i umowne przyjęte w celu zapobieżenia międzynarodowemu dostępowi do danych nieosobowych przechowywanych na terenie Unii lub ich przekazania administracji rządowej, w przypadku, gdy taki dostęp lub takie przekazanie skutkowałyby naruszeniem prawa Unii lub prawa krajowego danego państwa członkowskiego.

   - Dane przechowywane są wyłącznie na WCD TMPL lub Conpeek na terenie Polski
   - Szyfrowania transmisji (TLS 1.3) oraz SSL.
   - Dostawcy stosują klauzule zobowiązujące do nieprzekazywania danych poza UE bez uprzedniej zgody klienta

5. Informacje o usługach przetwarzania danych, które wiążą się z wysoce złożoną lub kosztowną zmianą dostawcy lub z niemożnością zmiany dostawcy bez znacznej ingerencji w dane, aktywa cyfrowe lub architekturę usługi.

   Nie dotyczy usługi Wirtualne Call Center.

Informacje dotyczące usługi przetwarzania danych: WIDEO ANALIZA

1. Informacje o istniejących procedurach zmiany dostawcy i przeniesienia usługi przetwarzania danych, w tym informacje o dostępnych metodach i formatach zmiany dostawcy i przeniesienia oraz o limitach i ograniczeniach technicznych znanych dostawcy usług przetwarzania danych.

   Klient ma prawo do zmiany dostawcy usługi Wideo Analiza na innego dostawcę usług lub do przeniesienia danych i zasobów cyfrowych do własnej infrastruktury. Należy zwrócić uwagę na charakter usług, a w szczególności zapis video w trybie ciągłym i możliwe duże ilości danych.

2. Informacje o strukturach danych i formatach danych oraz o stosownych normach i otwartych specyfikacjach w zakresie interoperacyjności, w których dostępne są dane eksportowalne

   W trakcie korzystania z usługi zbierane są następujące dane:

   - Pliki video, które Klient może pobrać samodzielnie na swoje zasoby, za pomocą posiadanych przez siebie narzędzi.

3. Jurysdykcja, której podlega infrastruktura ICT używana do przetwarzania danych w ramach ich poszczególnych usług

   Usługa podlega jurysdykcji Rzeczpospolitej Polskiej.

4. Środki techniczne, organizacyjne i umowne przyjęte w celu zapobieżenia międzynarodowemu dostępowi do danych nieosobowych przechowywanych na terenie Unii lub ich przekazania administracji rządowej, w przypadku, gdy taki dostęp lub takie przekazanie skutkowałyby naruszeniem prawa Unii lub prawa krajowego danego państwa członkowskiego.

   Wszystkie dane generowane przez nasze produkty skomunikowane w sposób bezpieczny i zgodny z obowiązującymi przepisami prawa. Dane te są przechowywane wyłącznie w lokalizacjach znajdujących się na terenie Unii Europejskiej.

   Zapewniamy wysoki standard bezpieczeństwa danych dzięki zastosowaniu nowoczesnych technologii zabezpieczających oraz ścisłemu przestrzeganiu procedur bezpieczeństwa.

   W zakresie udostępniania danych, zapewniamy, że:

   - Dane są udostępniane użytkownikom wyłącznie na terenie Unii Europejskiej.
   - Dane mogą być udostępniane osobom trzecim jedynie na wyraźny wniosek klientów.
   - Każde działanie związane z przekazywaniem danych jest starannie rejestrowane w naszym systemie, co umożliwia pełną przejrzystość i możliwość przeprowadzenia audytu w każdej chwili. Dzięki temu zapewniamy, że wszystkie operacje na danych są realizowane zgodnie z najwyższymi standardami ochrony danych osobowych i prywatności.

5. Informacje o usługach przetwarzania danych, które wiążą się z wysoce złożoną lub kosztowną zmianą dostawcy lub z niemożnością zmiany dostawcy bez znacznej ingerencji w dane, aktywa cyfrowe lub architekturę usługi.

   Nie dotyczy usługi Wideo Analiza

Niniejszy dokument realizuje obowiązek informacyjny wynikający z rozporządzenie parlamentu europejskiego i rady (UE) 2023/2854 z dnia 13 grudnia 2023 r w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych).