Security Whitepaper

Bezpieczeństwo informacji, Ochrona danych osobowych, Cyberbezpieczeństwo, AI

Stan na dzień 18.03.2026

Niniejszy dokument jest dostępny publicznie

Trans.eu Group S.A.

z siedzibą we Wrocławiu, posiadająca adres ul. Racławicka 2-4, 53-146 Wrocław, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego, której akta rejestrowe znajdują się w Sądzie Rejonowym dla Wrocławia - Fabrycznej we Wrocławiu VI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem 0000720763, NIP: 8942764658, REGON: 932920615, posiadająca kapitał zakładowy w wysokości 203.500,00 PLN, w pełni opłacony.

Wersje dokumentu

Wersja Nr	Data publikacji	Nazwa dokumentu	Wprowadzone zmiany
1.0	07.11.2023	Security Whitepaper	Brak - jest to pierwsza wersja dokumentu.
1.1	08.11.2023	Security Whitepaper	Punkt 6.1: nazwa aplikacji "Loads2DO" zmieniona na "Loads4Driver"
1.2	30.08.2024	Security Whitepaper	1. Zaktualizowano informacje o certyfikacie ISO 27001 2. Dodano sekcję „Autoryzacja użytkowników” 3. Zaktualizowano numerację rozdziałów i spis treści
1.3	05.03.2025	Security Whitepaper	1. Zaktualizowano sekcję “Przesyłanie danych” 2. Zaktualizowano sekcję “Wysoka dostępność” 3. Zaktualizowano sekcję “Centra danych — ogólna architektura hostingu” 4. Dodano sekcję “Polityka AI” 5. Poprawiono numerację stron
1.4	11.08.2025	Security Whitepaper	1. Zaktualizowano informacje o certyfikacie ISO 27001 2. Zaktualizowano wysokość kapitału spółki
1.5	01.11.2025	Security Whitepaper	1. Dodano sekcję “Bezpieczeństwo eCMR w ramach Platformy Trans.eu” 2. Zaktualizowano spis treści
1.6	18.03.2026	Security Whitepaper	1. Zaktualizowano informację o metodach uwierzytelniania

Wstęp

Trans.eu Group S.A. ("**Trans.eu**") dostarcza skalowalną platformę logistyczną, która łączy firmy spedycyjne, operatorów logistycznych, spedytorów i przewoźników. Została zaprojektowana z myślą o wysokiej dostępności i niezawodności, zapewniając narzędzia, które umożliwiają klientom wykonywanie szerokiej gamy zadań usprawniających ich procesy biznesowe.

Niniejszy dokument ma na celu przedstawienie podstawowej infrastruktury Trans.eu, w tym podejścia firmy do bezpieczeństwa, ochrony danych osobowych i wysokiej dostępności. Aby ułatwić jego zrozumienie, został on podzielony na sekcje wymienione w spisie treści.

W Trans.eu wierzymy, że bezpieczeństwo to nie stan, ale ciągłe dążenie do coraz lepszych rozwiązań mających na celu ochronę tego, co posiada wartość - w szczególności cenne dane naszych klientów. Dlatego często wdrażamy nowe rozwiązania bezpieczeństwa i aktualizujemy ten dokument. Jeśli jakiekolwiek informacje zawarte w nim nie są dla Ciebie wystarczające i/lub masz jakiekolwiek wątpliwości, skontaktuj się z nami - dołożymy wszelkich starań, aby rozwiać wszelkie obawy i wątpliwości dotyczące bezpieczeństwa.

Spis treści

1. Zarządzanie bezpieczeństwem danych 7
1.1. Certyfikat ISO 27001 7
1.2. Techniczne, organizacyjne i prawne środki bezpieczeństwa 8
1.3. Reguły i procedury 8
2. Audyty bezpieczeństwa 8
2.1. Audyty wewnętrzne i zewnętrzne 8
2.2. Automatyczne i tradycyjne metody audytu 9
2.3. Zakres audytów 9
2.4. Częstotliwość audytów 9
3. Rozwiązania w zakresie bezpieczeństwa systemu i dostępu do systemu 10
3.1. Ogólne 10
3.2. Centra danych — ogólna architektura hostingu 10
3.3. Przesyłanie danych 12
3.4. Wysoka dostępność 12
3.5. Kopie zapasowe danych i zabezpieczenia konfiguracji 13
3.6. Zarządzanie infrastrukturą 14
3.7. Zarządzanie użytkownikami wewnętrznymi i zewnętrznymi 14
4. Bezpieczeństwo sieci 15
4.1. Ogólne 15
4.2. Połączenie z Internetem 15
4.3. Rejestrowanie, monitorowanie i zarządzanie incydentami 15
5. Fizyczna kontrola dostępu 15
5.1. Fizyczna kontrola dostępu w centrach danych 15
5.2. Kontrola dostępu do pomieszczeń firmy 16
6. Dostęp dla klientów 17
6.1. Dostęp do Platformy Trans.eu 17
6.2. Autoryzacja użytkowników 17
6.3. Uwierzytelnianie wieloskładnikowe (MFA) 17
6.4. Zarządzanie kontami użytkowników i typ konta użytkownika (rola) 18
7. Dostęp dla pracowników 18
7.1. Procedury onboardingu i offboardingu 18
7.2. Zakres dostępu dla pracowników 18
7.3. Standardy dostępu pracowników 18
7.4. Praca zdalna chroniona siecią VPN 19
7.5. Uwierzytelnianie wieloskładnikowe pracowników (MFA) 19
8. Szyfrowanie danych 19
8.1. Wysokie standardy szyfrowania 19

8.2. Szyfrowanie podczas przesyłania danych 19
8.3. Szyfrowanie danych w spoczynku 20
9. Zarządzanie zmianami i poprawkami 20
9.1. Zarządzanie zmianami 20
9.2. Zarządzanie poprawkami 20
10. Kopie zapasowe 20
10.1. Częstotliwość 20
10.2. Lokalizacja 21
10.3. Obsługa 21
11. Serwery 21
11.1. Wsparcie 21
11.2. Aktualizacje i poprawki 21
12. Zarządzanie zdarzeniami i incydentami 21
12.1. Zarządzanie zdarzeniami 21
12.2. Zarządzanie incydentami 21
12.3. Kategorie zdarzeń i incydentów 22
13. Szkolenie pracowników w zakresie bezpieczeństwa 22
13.1. Onboarding 22
13.2. Odnowienie szkolenia 22
14. Zarządzanie bezpieczeństwem stron trzecich 23
14.1. Proces homologacji podwykonawców i dostawców oraz ocena ryzyka 23
14.2. Proces homologacji w zakresie zarządzania bezpieczeństwem klienta 23
15. Ciągłość działania i odzyskiwanie danych po awarii 23
15.1. Kopie zapasowe 23
15.2. Ciągłość działania 24
15.3. Odzyskiwanie danych po awarii 24
16. Bezpieczeństwo danych osobowych 24
16.1. Zgodność z RODO 24
16.2. Zasady przetwarzania danych osobowych, podstawy prawne przetwarzania 25
16.2.1. Zasady przetwarzania danych osobowych 25
16.2.1.1. Zasada legalności, rzetelności i przejrzystości 25
16.2.1.2. Zasada ograniczenia celu 25
16.2.1.3. Zasada minimalizacji danych 26
16.2.1.4. Zasada prawidłowości 26
16.2.1.5. Zasada ograniczenia przechowywania 26
16.2.1.6. Zasada integralności i poufności 27
16.2.1.7. Zasada rozliczalności 27
16.2.2. Co zapewniamy 27
16.2.3. Podstawy prawne przetwarzania danych 27
16.3. Prawa osób, których dane dotyczą 28

16.4. Obowiązek informacyjny 28
16.5. Ocena wpływu na ochronę danych 28
16.6. Środki bezpieczeństwa 28
16.7. Zgłaszanie naruszeń 28
16.7.1. Naruszenie ochrony danych 28
16.7.2. Naruszenie ochrony danych osobowych 28
16.7.3. Powiadomienie o naruszeniu ochrony danych osobowych 29
16.7.4. Sytuacje zidentyfikowane jako ryzyko naruszenia 29
16.7.5. Ocena ryzyka naruszenia 29
16.7.6. Naruszenie ochrony danych osobowych niepodlegające zgłoszeniu 30
16.7.7. Obowiązek zgłoszenia 30
16.7.8. Ocena ryzyka naruszenia 30
16.7.9. Powiadomienie osoby fizycznej 30
16.7.10. Dokumentacja 30
16.9. Eksport danych 31
17. Polityka AI 32
17.1. Integracja AI w Trans.eu 32
17.2. Zgodność i odpowiedzialne wykorzystanie AI 32
17.3. Etyczna AI i przejrzystość 32
17.4. Ocena ryzyka i minimalizacja zagrożeń związanych z AI 33
17.4.1. Kryteria oceny ryzyka AI 33
17.4.2. Strategie minimalizacji ryzyka 33
17.5. Narzędzia AI dla klientów 34
17.6. Ciągłe doskonalenie i przyszłość 34
18. Bezpieczeństwo eCMR w ramach Platformy Trans.eu 34
18.1. Charakterystyka rozwiązania eCMR 34
18.2. Model autoryzacji i zarządzania uprawnieniami 34
18.3. Widoczność i dostępność dokumentów 35
18.4. Podpis elektroniczny i potwierdzenie dostawy 35
18.5. Bezpieczeństwo i zgodność techniczna 36
18.6. Interfejsy i integracje 36
18.7. Zarządzanie incydentami bezpieczeństwa 36

1. Zarządzanie bezpieczeństwem danych

1.1. Certyfikat ISO 27001

Od 2016 roku Trans.eu posiada wdrożony System Zarządzania Bezpieczeństwem Informacji zgodny z normą ISO/IEC 27001. System podlega regularnym audytom i otrzymuje odpowiednią certyfikację. Wysoki standard przeprowadzanych audytów potwierdza renoma audytora certyfikującego - Dekra Certification Sp. z o.o., który posiada akredytację PCA (Polskiego Centrum Akredytacyjnego - krajowej jednostki akredytującej na terenie Rzeczypospolitej Polskiej) oraz jest członkiem IAF (International Accreditation Forum, Inc. - Multilateral Recognition Arrangement (MLA)).

Aktualny certyfikat można znaleźć tutaj: Certyfikat ISO 27001.

Trans.eu na bieżąco śledzi zmiany wprowadzane w ramach normy ISO 27001. Poniżej znajduje się lista certyfikatów ISO 27001 uzyskanych przez Trans.eu.

Tabela 1. Historia certyfikatów ISO 27001

Okres	Wersja ISO 27001	Zakres certyfikacji	Organ akredytujący
2016-2019	ISO/IEC 27001:2013	Dostarczanie rozwiązań informatycznych dla branż: transportowej, spedycyjnej i logistycznej	Dekra Certification GmbH
2019-2022	ISO/IEC 27001:2017	Dostarczanie rozwiązań informatycznych dla branż: transportowej, spedycyjnej i logistycznej	Dekra Certification GmbH
2022-2025	ISO/IEC 27001:2017	Dostarczanie rozwiązań informatycznych dla branż: transportowej, spedycyjnej i logistycznej	Dekra Certification GmbH
2024-2025	ISO/IEC 27001:2017	Dostarczanie rozwiązań informatycznych dla branż: transportowej, spedycyjnej i logistycznej	Dekra Certification Sp. z o.o.
2025-2028	ISO/IEC 27001:2022	Dostarczanie rozwiązań informatycznych dla branż: transportowej, spedycyjnej i logistycznej	Dekra Certification Sp. z o.o.

Aby uzyskać certyfikat ISO 27001, firma musi przejść szczegółowy audyt Systemu Zarządzania Bezpieczeństwem Informacji. Certyfikat ISO 27001 jest wydawany na 3 lata, jednak aby go zachować, firma musi co roku przechodzić audyty kontrolne SZBI.

1.2. Techniczne, organizacyjne i prawne środki bezpieczeństwa

W celu zapewnienia bezpieczeństwa informacji, prywatności danych i cyberbezpieczeństwa w Trans.eu wprowadzono i stosuje się szereg technicznych, organizacyjnych i prawnych środków bezpieczeństwa, z których większość została opisana w niniejszym dokumencie.

1.3. Reguły i procedury

Trans.eu stosuje politykę bezpieczeństwa informacji obejmującą jej wszystkich pracowników. Niniejsza polityka bezpieczeństwa informacji jest okresowo sprawdzana, zatwierdzana, przekazywana wszystkim pracownikom i jest zgodna z zalecanymi przez branżę standardami. Trans.eu posiada również formalny proces zarządzania ryzykiem związanym z bezpieczeństwem informacji, który ustala priorytety, dokumentuje i śledzi zidentyfikowane ryzyka aż do ich wyeliminowania. Audyty wewnętrzne są przeprowadzane regularnie w celu zapewnienia, że Trans.eu działa zgodnie z zasadami i wytycznymi dotyczącymi bezpieczeństwa informacji. Trans.eu posiada również politykę prywatności, która reguluje ochronę danych osobowych, w tym danych osobowych klientów (ochrona danych osobowych została szczegółowo opisana w punkcie 16. Bezpieczeństwo danych osobowych).

Istnieje formalny schemat klasyfikacji danych, który ma zastosowanie do danych klientów i określa poziom ochrony w zależności od klasyfikacji (np. publiczny, wewnętrzny, poufny itp.). Trans.eu zdefiniował procesy i technologię segregowania danych klientów w celu zapewnienia integralności i poufności. Istnieją również udokumentowane i zatwierdzone procesy oraz procedury zarządzania kluczami szyfrowania (np. PKI, certyfikat CA, dystrybucja i rotacja kluczy).

Trans.eu prowadzi aktualną i kompletną inwentaryzację sprzętu, maszyn wirtualnych, oprogramowania i aplikacji.

2. Audyty bezpieczeństwa

2.1. Audyty wewnętrzne i zewnętrzne

Trans.eu podlega regularnym audytom bezpieczeństwa. Audyty wewnętrzne są przeprowadzane co najmniej raz w roku w celu pomiaru zgodności, skuteczności i bezpieczeństwa (np. skanowanie bezpieczeństwa aplikacji oraz wewnętrzne audyty zgodności z normą ISO 27001). Wewnętrzne audyty zgodności z normą ISO 27001 przeprowadzane są przez certyfikowanych audytorów wewnętrznych. Co najmniej raz w roku przeprowadzane są również audyty zewnętrzne przez renomowane podmioty,

które potwierdzają jakość kontroli własną reputacją i profesjonalizmem (np. audyty bezpieczeństwa aplikacji, wewnętrznej infrastruktury IT i CRM przeprowadzane przez Securitum Audyty Sp. z o.o. Sp.k., audyt certyfikacyjny ISO 27001 przeprowadzony przez Dekra Certification Sp. z o.o.).

2.2. Automatyczne i tradycyjne metody audytu

Trans.eu zawsze dobiera najbardziej odpowiednią metodę audytu. O ile większość kontroli przeprowadzana jest w sposób tradycyjny (np. wewnętrzne i zewnętrzne audyty zgodności z normą ISO 27001, manualne audyty bezpieczeństwa realizowane przez Securitum Audyty Sp. z o.o. Sp.k.), wszędzie tam, gdzie jest to możliwe, stosowane są audyty automatyczne w celu zwiększenia częstotliwości przeprowadzonych kontroli (np. automatyczne skanowanie bezpieczeństwa aplikacji lub jej części (modułów)).

2.3. Zakres audytów

Trans.eu często przechodzi szereg audytów z uwzględnieniem SZBI, samej aplikacji i wszystkich elementów systemu. Audyty weryfikują zgodność z normą ISO 27001, czyli jak dobrze Trans.eu zarządza bezpieczeństwem przetwarzanych przez siebie informacji. Audyty bezpieczeństwa aplikacji i infrastruktury IT weryfikują stosowane techniczne środki bezpieczeństwa. Obejmują one skanowanie całej aplikacji i środowiska infrastruktury wewnętrznej w celu wykrycia oraz usunięcia/złagodzenia podatności, błędów i luk bezpieczeństwa. Składają się one m.in. z testów penetracyjnych (pentestów). Audyty bezpieczeństwa aplikacji obejmują całą Platformę Trans.eu, w tym jej środowisko, zintegrowane aplikacje oraz produkty i linie produktowe. Audyty bezpieczeństwa systemu obejmują każdy z elementów osobno oraz uwzględniają testy penetracyjne tych elementów.

2.4. Częstotliwość audytów

Wszystkie rodzaje audytów (w tym automatyczne i ręczne skanowanie oraz pentesty) są przeprowadzane co najmniej raz w roku, choć większość z nich odbywa się częściej - zwykle raz na trzy do sześciu miesięcy. Aby uzyskać certyfikat ISO 27001, firma musi przejść szczegółowy audyt SZBI. Certyfikat ISO 27001 jest wydawany na 3 lata, jednak aby go zachować, firma musi co roku przechodzić audyty kontrolne SZBI. Częstotliwość audytów bezpieczeństwa aplikacji i infrastruktury IT (zwłaszcza pentestów) wynosi od roku do 3 miesięcy. Aplikacja poddawana jest również statycznej analizie kodu, mającej na celu wykrycie podatności po każdej wprowadzonej zmianie (zawsze przed wdrożeniem na produkcję).

3. Rozwiązania w zakresie bezpieczeństwa systemu i dostępu do systemu

3.1. Ogólne

Trans.eu konsekwentnie stosuje i zarządza konfiguracjami bezpieczeństwa w swoich systemach, aplikacjach i urządzeniach sieciowych, a także posiada mechanizmy wykrywania i korygowania dryfu konfiguracji.

Stosowane są mechanizmy ochrony przed złośliwym oprogramowaniem, które są wdrażane na wszystkich naszych urządzeniach i są skonfigurowane do wykonywania skanowania i pobierania aktualizacji definicji z zaufanego źródła.

Wszystkie działające wersje systemów operacyjnych, wirtualizacji, sieci, oprogramowania pośredniczącego, baz danych i aplikacji w naszym środowisku są obsługiwane przez odpowiednich dostawców.

Stosowane są procesy i narzędzia do tworzenia kopii zapasowych informacji o klientach lub usługach, ochrony kopii zapasowych przed manipulacją oraz sprawdzona metodologia szybkiego przywracania informacji lub usług.

Trans.eu wykorzystuje procesy i narzędzia do śledzenia, kontrolowania, przeciwdziałania i poprawy użytkowania, przypisywania i konfigurowania uprawnień administracyjnych na komputerach, w sieciach i aplikacjach.

Trans.eu wykorzystuje mechanizmy służące do oddzielenia i ochrony sieci wewnętrznych przed sieciami niezaufanymi.

Trans.eu stosuje procesy mające na celu utrzymanie integralności konfiguracji sprzętu i oprogramowania, w tym wykrywanie i usuwanie błędów konfiguracji.

Trans.eu wdrożyła proces cyklu życia i bezpiecznej utylizacji sprzętu używanego w organizacji (serwery, stacje robocze, laptopy, telefony komórkowe lub tablety, urządzenia pamięci masowej USB itp.).

3.2. Centra danych — ogólna architektura hostingu

Trans.eu jest hostowana w dwóch głównych centrach danych w Europie. Jedno z nich znajduje się w Polsce i jest obsługiwane przez firmę Talex (https://www.talex.pl/), partnera w zakresie usług data center w Europie Środkowo-Wschodniej. Drugi z nich działa w oparciu o AWS firmy Amazon, najbardziej wszechstronnej i szeroko stosowanej platformy chmurowej na świecie.

Obie lokalizacje wybrane dla hostingu Trans.eu to najnowocześniejsze centra przetwarzania danych, z silnymi modelami bezpieczeństwa fizycznego i logicznego, stałym monitoringiem, rejestrami aktywności, CCTV itp. Struktura obu centrów danych jest zgodna z najlepszymi dostępnymi praktykami.

Talex spełnia wymagania Data Center Operations Standard; Certyfikacja DCOS-4 zapewnia wysoką dostępność usług świadczonych przez oba centra danych oraz gwarantuje, że procedury operatora są poprawnie zdefiniowane, przetestowane, udokumentowane, a ich jakość i adekwatność jest stale monitorowana i ulepszana. To centrum danych posiadają system SZBI zgodny z normą ISO/IEC 27001.

Wirtualne centrum danych utrzymywane w ramach platformy chmurowej Amazon AWS, przeznaczone dla lżejszej, ale silnie skalowalnej części Trans.eu, która obsługuje stale zmieniające się wzorce obciążenia i sieci, jest częścią AWS Global Cloud Infrastructure. Więcej informacji na ten temat można znaleźć na stronach internetowych Amazon AWS, korzystając z linków zamieszczonych na końcu tej sekcji (Tabela 2).

Centra danych Talex i AWS połączone są ze sobą dedykowanym protokołem MPLS i tunelami VPN. Ponadto oba centra danych posiadają dedykowane, publicznie dostępne endpointy powiązane logicznie jako jeden, jednolity entry point dla klientów Platformy Trans.eu (osobno dla klientów detalicznych i korporacyjnych). Dzięki temu Platforma Trans.eu jest gotowa na wykorzystanie wszystkich dostępnych funkcjonalności CDN i geolokalizacji oraz jest odporna na większość krytycznych awarii w routingu lub przerw w dostawie Internetu.

Tabela 2. Centra danych

Centrum danych	**TALEX**	**AWS**
Usługodawca	**"Talex" S.A.** ul. Karpia 27D 61-619 Poznań Polska, UE KRS: 0000048779	**Amazon Web Services EMEA SARL** 38 Avenue John F. Kennedy L-1855 Luksemburg Luksemburg, UE RCS: B186284
Usługi	https://www.talex.pl/en/services/collocation/	https://aws.amazon.com/compliance/data-center/data-centers/
Systemy kontroli	https://www.talex.pl/en/services/talex-data-center/	https://aws.amazon.com/compliance/data-center/controls/

	https://www.talex.pl/en/	https://aws.amazon.com/about-aws/global-infrastructure/
Lokalizacje	Unia Europejska https://www.talex.pl/en/services/talex-data-center/	Unia Europejska https://aws.amazon.com/about-aws/global-infrastructure/

3.3. Przesyłanie danych

Podstawowym komponentem w obu centrach danych odpowiedzialnym za właściwą komunikację i bezpieczeństwo danych w Trans.eu jest warstwa sieciowa. Mimo że network stack i przepływ danych w środowisku chmurowym AWS różni się od odpowiadającej mu implementacji w centrum danych Talex, oba mają te same rygorystyczne zasady dotyczące zabezpieczenia, rozdzielenia control i data plane, warstw sieci i redundancji.

W obu lokalizacjach konfiguracje sieci wykorzystują granularne podsieci (w zależności od wyznaczonej funkcji danej podsieci), warstwy sieci (używane do wymuszania kierunku ruchu IP i segmentacji), obie wspierane przez odpowiednie reguły routingu i zapory. Oba centra danych korzystają z wielu połączeń ISP do obsługi wysokiej przepustowości sieci, równoważenia obciążenia i redundancji.

W lokalizacji Talex utrzymywane są osobne segmenty DMZ i LAN, z których każdy jest chroniony redundantnymi zaporami sieciowymi. Zastosowane rozwiązania pozwalają na zwiększenie dostępności usług Trans.eu. Cały ruch IP w centrum danych Talex jest monitorowany zarówno w sposób bezpośredni, jak i pośredni.

Wirtualne centrum danych w AWS izoluje komponenty Trans.eu na poziomie VPC. Load balancery aplikacji i sieci stanowią, obok wbudowanych w AWS zabezpieczeń, pierwszy poziom ochrony. Cały ruch sieciowy w AWS jest monitorowany.

3.4. Wysoka dostępność

Trans.eu została stworzona z myślą o wysokiej dostępności, począwszy od projektów zarówno infrastruktury, jak i aplikacji, czyniąc je komplementarnymi pod względem wspólnych celów, ale nadal od siebie oddzielonymi. Dzięki takiemu podejściu oprogramowanie, projekty warstw obliczeniowych, danych i komunikacji mogą być opracowywane niezależnie, co pozwala na uruchamianie usług Trans.eu w trybie wysokiej dostępności niezależnie od centrum danych, w którym miały działać.

W obu lokalizacjach centrów danych stosuje się wielorakie, a czasami specyficzne dla danej infrastruktury rozwiązania techniczne w celu osiągnięcia wysokiej dostępności.

Oba centra danych korzystają z usług wielu firm ISP w celu uzyskania dostępu do Internetu i widoczności publicznej. Redundantne są również połączenia międzysystemowe między wszystkimi lokalizacjami.

Wszystkie punkty końcowe usług, niezależnie od ich lokalizacji, są dostępne za pośrednictwem pojedynczego logicznego punktu końcowego zapytania za pośrednictwem warstwy wykrywania usług, z publicznymi endpointami uzupełnionymi w warstwie brzegowej o dodatkowe load balancery ISO/OSI warstwy 4 i warstwy 7, a ponadto o CDN.

W lokalizacji Talex usługi są dostępne jako maszyny wirtualne działające na wysokowydajnych i wysoce dostępnych farmach pamięci masowych i hiperwizorów, rozmieszczonych w wielu połączonych ze sobą szafach serwerowych wyposażonych w redundantne zasilacze, urządzenia komunikacyjne, łącza itp. Zastosowane rozwiązania pozwalają na nadzorowanie i przewidywanie wszystkich niezbędnych aktualizacji sprzętu i funkcji, które uznają za konieczne w ciągu najbliższych 3-6 miesięcy, co zapewnia więcej wolnej przestrzeni na dodatkowe obciążenie lub nieprzewidzianą awarię sprzętu.

W AWS, gdzie większość usług musi mierzyć się ze stale zmieniającymi się wzorcami obciążenia i sieci, jednocześnie uwzględniając specyfikę cloud computingu, komponenty Trans.eu korzystają z wielu obszarów dostępności, grup automatycznego skalowania zasobów, mocy obliczeniowej i automatycznego skalowania aplikacji. Połączenie wszystkich tych cech pozwala na szybkie i odporne na awarie skalowanie wielu usług w tym samym czasie, zgodnie z aktualnymi wymaganiami użytkowania, bez żadnych skutków ubocznych dla reszty systemu. Metody te pozwalają na zastosowanie takiej mechaniki predykcji i automatyzacji, jaką może dostarczyć wybrany dostawca chmury.

Wszystkie komponenty Trans.eu są monitorowane 24 godziny na dobę, 7 dni w tygodniu, a dedykowany zespół jest gotowy do działania, gdy z jakiegoś powodu automatyczna naprawa lub przełączanie awaryjne nie przywróci wadliwie działających komponentów do wymaganego poziomu operacyjnego.

Wszystkie systemy sieciowe i serwerowe wykorzystują układy redundantne.

3.5. Kopie zapasowe danych i zabezpieczenia konfiguracji

Wszystkie komponenty aplikacji Trans.eu zostały zaprojektowane i zaimplementowane tak, aby były całkowicie bezstanowe. Pozwoliło to ograniczyć operacje tworzenia kopii

zapasowych do baz danych i współdzielonych systemów plików, co uprościło proces planowania, polityki przechowywania i testy odzyskiwania danych po awarii.

Wszystkie kopie zapasowe danych z każdego centrum danych podlegają zasadom przechowywania między lokalizacjami i poza siedzibą firmy, co pozwala grupie zadaniowej Trans.eu na pełne odzyskanie danych w przypadku krytycznej awarii w jednym z naszych centrów danych.

Dodatkowo, dzięki temu, że cała infrastruktura jest zarządzana przez configuration managerów i narzędzi infrastructure-as-code za pomocą nowoczesnych rozwiązań dla repozytoriów kodu, systemy Trans.eu mogą być ponownie wdrożone w zupełnie nowym centrum danych w momencie, gdy korzystanie z danej lokalizacji nie będzie już możliwe.

3.6. Zarządzanie infrastrukturą

Cała infrastruktura Trans.eu jest bezpośrednio zarządzana przez rozwiązania typu infrastructure-as-code i configuration managerów. W związku z tym posiadanie całej konfiguracji wersjonowanej i przechowywanej w kodzie pozwoliło na drastyczne skrócenie czasu wdrażania i wycofywania wersji, wraz z automatyczną walidacją, testowaniem i dostarczaniem nowych usług przy użyciu pipeline'ów CI/CD. Umożliwiło to również wdrożenie tych samych protokołów bezpieczeństwa we wszystkich komponentach Trans.eu, praktycznie eliminując możliwość wystąpienia błędu ludzkiego.

3.7. Zarządzanie użytkownikami wewnętrznymi i zewnętrznymi

Bezpośredni dostęp do infrastruktury dla każdej grupy użytkowników — programistów i grupy operations task force — jest obsługiwany zarówno przez polityki bezpieczeństwa sieci, jak i rozproszone usługi katalogowe. Wszystkie centra danych korzystają z kontroli dostępu typu fine-grade, zapewnianej przez zintegrowane rozwiązania LDAP.

Dla każdej grupy użytkowników lub na poziomie pojedynczego użytkownika stosowane są odrębne polityki bezpieczeństwa, w zależności od poziomu zaufania, obszaru odpowiedzialności i zasady najmniejszego uprzywilejowania. Podczas gdy zespół operacyjny zwykle ma dostęp do większości, jeśli nie wszystkich składników systemu Trans.eu, zarówno na poziomie kontroli, jak i danych, zespoły programistyczne dysponują jedynie określonymi endpointami z dostępem tylko do odczytu.

Zdalny dostęp do wszystkich zasobów obliczeniowych i danych, w tym serwerów, klastrów kontenerów, repozytoriów kodu itp., jest zabezpieczony przez rozwiązania VPN o bardzo restrykcyjnych zasadach dostępu zintegrowanych z rozwiązaniami Deep Packet Inspection (DPI). Dostęp VPN do wszystkich krytycznych zasobów Trans.eu jest

przyznawany tylko ograniczonej grupie użytkowników (dział operacyjny, zespół dyżurny) i jest stale monitorowany.

4. Bezpieczeństwo sieci

4.1. Ogólne

Systemy są chronione przed atakami DDoS i brute force.

Stosowana jest odpowiednia segmentacja sieci.

Jeśli konieczna jest zdalna administracja, odbywa się ona za pośrednictwem bezpiecznych kanałów komunikacji. Jest ona realizowana przy użyciu wysokich standardów szyfrowania.

Wykorzystywana jest szyfrowana komunikacja z podwykonawcami (np. zewnętrznymi dostawcami usług w zakresie obsługi centrów danych). Jest ona realizowana przy użyciu wysokich standardów szyfrowania (Sekcja 8. Szyfrowanie danych).

4.2. Połączenie z Internetem

W każdym centrum danych dostępnych jest wiele połączeń internetowych. Wszelkie awarie wykrywane są automatycznie. Jeśli podstawowe połączenie zostanie przerwane, ruch jest przekierowywany do drugiego łącza internetowego (tzw. failover).

4.3. Rejestrowanie, monitorowanie i zarządzanie incydentami

Infrastruktura jest monitorowana 24/7 (dostępność usług i zasobów). Wewnętrzna reakcja na ataki i/lub inne incydenty związane z bezpieczeństwem jest bardzo szybka. Monitorowanie logów i ocena źródeł danych (stan systemu, błędne próby uwierzytelnienia) odbywa się regularnie. Trans.eu wdrożyła również proces/technologię w celu zapewnienia, że rejestry zdarzeń (np. dla systemów operacyjnych, sieci, baz danych, aplikacji itp.) są odporne na ingerencję.

5. Fizyczna kontrola dostępu

5.1. Fizyczna kontrola dostępu w centrach danych

Szczegółowe informacje na temat fizycznej kontroli dostępu w każdym z centrów danych, o których mowa w punkcie 3.1 można uzyskać w tych centrach danych – np. na ich stronach internetowych, o których mowa w tabeli 2 (Sekcja 3.2. Centra danych —

ogólna architektura hostingu). Wszystkie centra danych (oprócz innych fizycznych kontroli dostępu) zapewniają:

Lokalizacja centrum danych

- Nadzór wideo na zewnątrz centrum danych.
- Monitoring wideo wewnątrz centrum danych (w pomieszczeniach zamkniętych i szafach serwerowych).
- Monitoring budynków.
- Systemy antywłamaniowe.
- Ochrona 24x7x365 kontroluje dostęp do każdego budynku.
- Recepcja z wymaganym logowaniem dla gości.
- Mury/ogrodzenia otaczające budynki.
- Dostęp do parkingu dla pracowników lub gości jest ograniczony szlabanami i/lub ochroną.

Budynki centrów danych

- Budynki bez okien.
- Oddzielne strefy bezpieczeństwa fizycznego dla obszarów ogólnych, obszarów dostępnych dla klientów i centrum danych.
- Oddzielnie zamykane szafy serwerowe z możliwością zastosowania niestandardowych zamków i kluczy.

Dostęp do centrum danych

- Wieloskładnikowe zabezpieczenia do przyznawania dostępu, rejestrowane.
- Zarządzanie kluczami i dokumentacją posiadaczy kluczy.
- Elektroniczny system odczytu kart dostępu.
- Fizyczny dostęp do sprzętu przetwarzającego dane mają tylko osoby upoważnione, z wiedzą z zakresu bezpieczeństwa.
- Goście wchodzący do budynków są zawsze eskortowani.
- Dostęp do parkingu dla pracowników lub gości jest ograniczony przez szlaban i/lub ochroniarza.

5.2. Kontrola dostępu do pomieszczeń firmy

Fizyczne mechanizmy kontroli mające na celu zapobieganie nieautoryzowanemu dostępowi do dedykowanych obszarów roboczych klienta, między innymi:

- Dostęp do pomieszczeń Trans.eu jest ograniczony.
- Dostęp do pomieszczeń Trans.eu jest kontrolowany za pomocą kluczy elektronicznych i tradycyjnych.
- Dostęp do pomieszczeń biurowych Trans.eu jest chroniony drzwiami wyposażonymi w kontrolę dostępu.
- Goście wchodzący na teren Trans.eu są zawsze identyfikowani, rejestrowani i eskortowani.
- Obiekty Trans.eu i ich otoczenie monitorowane są kamerami CCTV.

6. Dostęp dla klientów

6.1. Dostęp do Platformy Trans.eu

Klienci mogą uzyskać dostęp do Platformy Trans.eu za pośrednictwem:

- przeglądarki internetowej (polecamy Google Chrome) pod adresem www.platform.trans.eu;
- aplikacja na Androida/iOS: Loads2GO i Loads4Driver;
- API (więcej na: https://www.trans.eu/api/).

6.2. Autoryzacja użytkowników

Każdy Klient (firma) ubiegający się o dostęp do Platformy Trans.eu musi przejść proces autoryzacji. Proces ten odbywa się w oparciu o regularnie weryfikowane i aktualizowane procedury i ma na celu wyeliminowanie potencjalnych zagrożeń dla i ze strony przyszłych kontrahentów firmy, m.in:

- fikcyjne dane - proces autoryzacji ma na celu sprawdzenie, czy wszystkie informacje o firmie Klienta i sposobie prowadzenia przez niego działalności gospodarczej są rzeczywiste i aktualne;
- niebezpieczne powiązania - proces autoryzacji ma na celu upewnienie się, że nowy Klient rejestrujący się na Platformie Trans.eu nie jest osobiście lub finansowo powiązany z byłym Klientem, który stanowił zagrożenie dla innych użytkowników Platformy;
- podszywanie się pod firmę - proces autoryzacji ma na celu sprawdzenie, czy osoby rejestrujące firmę jako Klienta na Platformie Trans.eu są faktycznie upoważnione do jej formalnej reprezentacji, a sama firma jest działającym przedsiębiorstwem, formalnie zarejestrowanym w kraju pochodzenia.

Proces autoryzacji sprawdza również, czy firma próbująca uzyskać dostęp do Platformy Trans.eu działa na rynku logistycznym (a nie na rynku niezwiązanym z logistyką).

6.3. Uwierzytelnianie wieloskładnikowe (MFA)

Aby uzyskać dostęp do Platformy Trans.eu, wszyscy Klienci muszą korzystać przynajmniej z uwierzytelniania dwuskładnikowego (2FA - two-factor authentication) przy użyciu wybranej metody (e-mail, SMS, hasło jednorazowe, dedykowana aplikacja).

Istnieje również udokumentowana i skuteczna polityka dotycząca haseł dla użytkowników.

6.4. Zarządzanie kontami użytkowników i typ konta użytkownika (rola)

Firma może zarządzać kontami swoich pracowników, tworząc i blokując powiązane konta oraz wybierając jego odpowiedni typ dla różnych ról pracowników.

7. Dostęp dla pracowników

7.1. Procedury onboardingu i offboardingu

Trans.eu wdrożyła procedury onboardingu i offboardingu, które obejmują udzielanie i odbieranie dostępu do danych i informacji przetwarzanych przez Trans.eu.

7.2. Zakres dostępu dla pracowników

Pracownicy uzyskują dostęp do danych i informacji przetwarzanych przez Trans.eu zgodnie z wewnętrznym regulaminem, który określa zakres danych i informacji dostępnych dla każdego członka personelu w zależności od pełnionej roli, zakresu obowiązków itp. Zasady te mają zastosowanie zarówno do nowo zatrudnionych, jak i przeniesionych pracowników. Trans.eu ma również zdefiniowaną politykę zarządzania dostępem uprzywilejowanym.

7.3. Standardy dostępu pracowników

Trans.eu spełnia następujące standardy:

- uprawnienia do systemów i sieci są ograniczone tylko do tych osób, które potrzebują tego dostępu do wykonywania swoich obowiązków służbowych;
- dostęp jest odbierany natychmiast, gdy nie jest już potrzebny;
- wnioski o dostęp są odpowiednio zatwierdzane przed ich udzieleniem;
- przeglądy dostępu są przeprowadzane okresowo.

Dostęp indywidualnego użytkownika / administratora jest logowany przy wejściu do systemu i / lub firmy.

Istnieje udokumentowany zestaw zasad, który opisuje proces administrowania kontami użytkowników wewnętrznych. Jest to zestaw standardowych i udokumentowanych procedur z jasno zdefiniowanymi rolami i obowiązkami w zakresie zapewniania dostępu, w tym nowych pracowników, przeniesień i zwolnień dla wszystkich członków personelu. Proces zarządzania dostępem obejmuje zarządzanie nieaktywnymi kontami użytkowników.

Istnieje również udokumentowana i skuteczna polityka haseł dla użytkowników wewnętrznych.

7.4. Praca zdalna chroniona siecią VPN

Podczas pracy zdalnej z dowolnego miejsca poza biurem personel Trans.eu korzysta z sieci VPN w celu uzyskania bezpiecznego dostępu do danych użytkowników/klientów.

7.5. Uwierzytelnianie wieloskładnikowe pracowników (MFA)

Aby uzyskać dostęp do systemów i danych Trans.eu, wszyscy pracownicy firmy muszą korzystać co najmniej z uwierzytelniania dwuskładnikowego (2FA - two-factor authentication).

8. Szyfrowanie danych

8.1. Wysokie standardy szyfrowania

Trans.eu wykorzystuje wysokie standardy szyfrowania: Advanced Encryption Standard (AES).

8.2. Szyfrowanie podczas przesyłania danych

W zależności od przypadku, przesyłane dane są szyfrowane przy użyciu odpowiedniej metody:

Tabela 3. Szyfrowanie podczas przesyłania danych

Kontekst	Technologia/metoda szyfrowania
Plik dołączony do wiadomości e-mail	Plik PDF / Excel / Word / ZIP itp. lub folder zabezpieczony hasłem
Systemy i dane, do których personel uzyskuje zdalny dostęp w celach służbowych Korzystanie z chmury	VPN
Dostęp użytkowników do Platformy	Protokół TLS

8.3. Szyfrowanie danych w spoczynku

Wszystkie dane kopii zapasowych oraz dyski twarde, w tym urządzenia mobilne (np. telefony, laptopy) są szyfrowane przy użyciu zaawansowanych standardów szyfrowania (AES).

9. Zarządzanie zmianami i poprawkami

9.1. Zarządzanie zmianami

Istnieje opracowany i udokumentowany proces zarządzania zmianami. Wnioski o zmianę są dokumentowane i przechowywane, zatwierdzane przez odpowiedniego przedstawiciela biznesowego, oceniany jest potencjalny wpływ na biznes. Zmiany są zawsze testowane w celu określenia oczekiwanych rezultatów. Trans.eu wykorzystuje osobne środowiska (produkcyjne i nieprodukcyjne) w procesie zarządzania zmianami. Zmiany są weryfikowane w celu zapewnienia, że nie zagrażają one środkom kontroli bezpieczeństwa.

Istnieje standardowy, formalny i udokumentowany proces zarządzania zmianami IT w celu zarządzania i kontroli zmian w systemie informatycznym Trans.eu. Proces ten wymaga formalnego zatwierdzenia wszystkich zmian. Zawiera on również jasny opis zmiany, jej konsekwencje, plan testów, plan wycofania zmiany, jej harmonogram oraz status.

9.2. Zarządzanie poprawkami

Trans.eu wdrożyła bezpieczny proces wytwarzania oprogramowania. Istnieją zasady i procedury, które zapobiegają wykorzystywaniu danych produkcyjnych klienta w środowiskach nieprodukcyjnych, takich jak systemy stacjonarne pracowników Trans.eu lub systemy wykorzystywane do developmentu, testowania lub QA. Trans.eu posiada również proces monitorowania i stosowania poprawek w systemach i aplikacjach. Proces zarządzania poprawkami jest opracowany i udokumentowany. Poprawki zawsze podlegają testom w celu sprawdzenia oczekiwanych rezultatów.

10. Kopie zapasowe

10.1. Częstotliwość

Ze względu na dynamiczny charakter Platformy Trans.eu, kopie zapasowe danych są wykonywane często w celu zabezpieczenia danych klientów i Trans.eu.

10.2. Lokalizacja

Kopie zapasowe danych są przechowywane offline i niezależnie od lokalizacji serwerów

10.3. Obsługa

Proces tworzenia kopii zapasowej obejmuje okresowe przywracanie danych i testowanie w celu zapewnienia dostępności i integralności danych objętych kopią zapasową. Trans.eu posiada proces monitorowania i odzyskiwania danych po awariach przy tworzeniu kopii zapasowych.

11. Serwery

11.1. Wsparcie

Istnieją umowy dotyczące pomocy technicznej dla odpowiedniego oprogramowania i sprzętu innych firm używanego w infrastrukturze serwerowej.

11.2. Aktualizacje i poprawki

Nowe aktualizacje i poprawki oprogramowania o krytycznym znaczeniu wydane przez dostawców oprogramowania/sprzętu są instalowane na naszych serwerach Trans.eu krótko po ich wydaniu. Aktualizacje i poprawki oprogramowania są najpierw testowane w oddzielnym środowisku, zanim serwery zostaną zaktualizowane lub otrzymają poprawki.

12. Zarządzanie zdarzeniami i incydentami

12.1. Zarządzanie zdarzeniami

Wprowadzono regularny monitoring i przegląd zdarzeń. Wszystkie odpowiednie typy zdarzeń (np. awaria systemu, usunięcie obiektu, niepoprawne hasło) są rejestrowane i przechowywane przez określony czas.

12.2. Zarządzanie incydentami

Proces zarządzania incydentami związanymi z bezpieczeństwem jest opracowany i udokumentowany. Trans.eu posiada formalną strategię zarządzania incydentami i problemami, która obejmuje procedury komunikacji i eskalacji. Ponadto Trans.eu śledzi i monitoruje zdarzenia związane z bezpieczeństwem informacji, aby upewnić się, że są one przeglądane, priorytetyzowane, przypisywane i naprawiane w odpowiednim czasie.

12.3. Kategorie zdarzeń i incydentów

Zdarzenia uznane za zagrożenie dla bezpieczeństwa można podzielić następująco:

- zdarzenie, które nie jest incydentem, tj. nie narusza bezpieczeństwa żadnych danych i/lub informacji;
- incydent związany z cyberbezpieczeństwem, tj. zdarzenie obejmujące naruszenie bezpieczeństwa systemów informatycznych;
- incydent RODO, tj. zdarzenie obejmujące naruszenie bezpieczeństwa danych osobowych;
- incydent ISO, tj. zdarzenie obejmujące naruszenie bezpieczeństwa danych i/lub informacji.

Zdarzenie może stanowić jeden, dwa, wszystkie lub żaden z wyżej wymienionych rodzajów incydentów. Dlatego zdarzenia są analizowane w różnych aspektach, aby zapewnić weryfikację wszystkich potencjalnych wymiarów bezpieczeństwa i dokładną reakcję na dane zdarzenie.

Niektóre zdarzenia nie stają się incydentami, ale ujawniają potencjalne zagrożenie (np. luki w zabezpieczeniach, defekty, itp.) i są odpowiednio obsługiwane.

Wpływ incydentu na bezpieczeństwo jest oceniany w czterostopniowej skali: niski, średni, wysoki oraz krytyczny, na co zapewniona jest odpowiednia reakcja.

13. Szkolenie pracowników w zakresie bezpieczeństwa

13.1. Onboarding

Proces onboardingu nowych pracowników obejmuje szkolenia z zakresu bezpieczeństwa informacji i ochrony danych osobowych.

13.2. Odnowienie szkolenia

Szkolenie z zakresu bezpieczeństwa można odnowić na wewnętrznej platformie e-learningowej. Zasady bezpieczeństwa są również powtarzane podczas różnych audytów wewnętrznych i za każdym razem, gdy są usprawniane.

14. Zarządzanie bezpieczeństwem stron trzecich

14.1. Proces homologacji podwykonawców i dostawców oraz ocena ryzyka

Nasi podwykonawcy i dostawcy przechodzą proces homologacji i oceny ryzyka w celu zapewnienia, że spełniają wymogi prawne oraz wymogi bezpieczeństwa adekwatne do danych i informacji, do których mogą mieć dostęp. Proces homologacji i ocena ryzyka mają miejsce przed zawarciem umowy z danym podwykonawcą i/lub dostawcą i są regularnie ponawiane w trakcie trwania umowy.

14.2. Proces homologacji w zakresie zarządzania bezpieczeństwem klienta

W celu zapewnienia bezpieczeństwa w zakresie relacji i transakcji biznesowych nasi klienci muszą przejść procesy weryfikacji i autoryzacji opisane w Regulaminie Platformy Trans.eu (dostępnym pod adresem: https://www.trans.eu/pl/regulations/). Proces autoryzacji jest przeprowadzany zgodnie z wewnętrznymi procedurami autoryzacji (procedury te stanowią część ściśle poufnej wewnętrznej dokumentacji bezpieczeństwa). Bez autoryzacji klient nie ma dostępu do Platformy Trans.eu. W razie konieczności (np. naruszenie Regulaminu Platformy Trans.eu) klient może zostać zobowiązany do ponownego poddania się procesowi autoryzacji (tj. procesowi ponownej autoryzacji - reautoryzacji).

Dzięki tym procesom Trans.eu może udostępnić Platformę Trans.eu tylko zweryfikowanym firmom. Procesy te są m.in. środkami minimalizującymi oszustwa. Trans.eu tworzy coraz bezpieczne środowisko dla użytkowników platformy Trans.eu.

15. Ciągłość działania i odzyskiwanie danych po awarii

15.1. Kopie zapasowe

Wszystkie dane Platformy Trans.eu oraz inne dane przetwarzane w wewnętrznej infrastrukturze Trans.eu są archiwizowane i szyfrowane (pkt 8. Szyfrowanie danych) na oddzielnym serwerze w fizycznie odseparowanym centrum danych. Kopie zapasowe są wykonywane z dużą częstotliwością.

Polityka tworzenia kopii zapasowych obejmuje:
- wszystkie systemy produkcyjne;
- wszystkie środowiska: test, staging i development;
- wszystkie inne dane.

Kopie zapasowe są zapisywane w zaszyfrowanej formie w bezpiecznej i stabilnej usłudze przechowywania danych. Wybrana lokalizacja kopii zapasowej zawsze różni się od lokalizacji serwera produkcyjnego.

Kopie zapasowe są stale monitorowane poprzez porównywanie wersji, aby upewnić się, że mają podobny rozmiar. Dzięki temu możemy szybko zidentyfikować wszelkie problemy związane z kopiami zapasowymi.

15.2. Ciągłość działania

Trans.eu posiada wiele biur w różnych krajach UE, przy czym główne z nich znajduje się w dwóch odrębnych lokalizacjach we Wrocławiu, w Polsce. W żadnym z tych biur nie istnieje krytyczna infrastruktura danych. Trans.eu jest w pełni zdolna do normalnej działalności, nawet jeśli którekolwiek z tych biur zostanie dotknięte awariami. Wszystkie operacje mogą wtedy być wykonywane zdalnie przez pracowników Trans.eu.

15.3. Odzyskiwanie danych po awarii

Uszkodzenie sprzętu dowolnej instancji Trans.eu można naprawić w odpowiednim czasie.

Cel czasu odzyskiwania (Recovery time objective)
Cel czasu odzyskiwania polega na przywróceniu działania Platformy Trans.eu po poważnej awarii infrastruktury serwerowej w odpowiednim czasie lub szybciej, jeśli uszkodzony został tylko sam sprzęt serwerowy.

Cel punktu odzyskiwania (Recovery point objective)
Cel punktu odzyskiwania jest ustawiony tak, aby odpowiadał aktualnemu statusowi danych.

16. Bezpieczeństwo danych osobowych

16.1. Zgodność z RODO

Ochrona danych osobowych naszych klientów i pracowników jest dla Trans.eu priorytetem.

W związku z tym, nasza Spółka dokłada wszelkich starań, aby spełnić wymogi 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, (dalej: RODO).

Nasze nieustanne działania w zakresie zgodności z przepisami opierają się na istniejących inwestycjach w ochronę prywatności, poufności, zapewnienie bezpieczeństwa i wdrożenie procedur operacyjnych niezbędnych do zapewnienia zgodności z RODO i innymi obowiązującymi przepisami. Trans.eu, działając zarówno jako Administrator, jak i podmiot przetwarzający dane, rozumie obowiązki wynikające z przestrzegania RODO.

Jeśli chcesz poznać szczegóły i zasady przetwarzania Twoich danych osobowych przez Trans.eu, zapoznaj się z **NASZĄ POLITYKĄ PRYWATNOŚCI**, dostępną pod adresem: https://www.trans.eu/en/privacy-policy/ oraz **Regulaminem Platformy Trans.eu**, dostępnym pod adresem: https://www.trans.eu/en/regulations/.

Ponadto, jeśli chcesz poznać szczegółowe informacje na temat wykorzystywania plików cookies przez Trans.eu, znajdziesz je w **Polityce dotyczącej plików cookie**, dostępnej na stronie internetowej: https://www.trans.eu/en/cookie-policy-eu/.

16.2. Zasady przetwarzania danych osobowych, podstawy prawne przetwarzania

16.2.1. Zasady przetwarzania danych osobowych

16.2.1.1. Zasada legalności, rzetelności i przejrzystości

Spółka zapewnia realizację zasady, o której mowa w art. 5 ust. 1 lit. a RODO, dotyczącej przetwarzania danych zgodnie z prawem, rzetelnie i w sposób przejrzysty poprzez zapewnienie podstawy prawnej przetwarzania oraz realizację praw osób fizycznych, w tym w szczególności informowanie osób fizycznych o przetwarzaniu ich danych zgodnie z wymogami RODO. W tym celu Spółka, w ramach swoich wewnętrznych procedur, zapewnia wdrożenie tej zasady.

16.2.1.2. Zasada ograniczenia celu

Spółka zapewnia realizację zasady zbierania danych wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz nieprzetwarzania ich dalej w sposób niezgodny z tymi celami, tj. zasady, o której mowa w art. 5 ust. 1 lit. b RODO. W tym celu Spółka, w ramach swoich wewnętrznych procedur, zapewnia realizację tej zasady, w szczególności poprzez zapewnienie

odpowiedniego nadzoru w tym zakresie, z uwzględnieniem ról i zadań Inspektora Ochrony Danych.

16.2.1.3. Zasada minimalizacji danych

Spółka zapewnia realizację zasady minimalizacji danych, o której mowa w art. 5 ust. 1 lit. c RODO, poprzez przetwarzanie danych, które są odpowiednie, stosowne oraz ograniczone do celów przetwarzania. W tym celu w Spółce funkcjonują wewnętrzne procesy mające na celu egzekwowanie tej zasady, w tym w szczególności uwzględnianie wymogów minimalizacji danych przy opracowywaniu nowych i modyfikowaniu istniejących procesów i systemów w ramach identyfikacji ryzyk operacyjnych.

16.2.1.4. Zasada prawidłowości

Spółka zapewnia realizację zasady, o której mowa w art. 5 ust. 1 lit. d RODO, zgodnie z którą dane powinny być prawidłowe i w razie potrzeby aktualizowane. Spółka podejmie wszelkie uzasadnione kroki w celu zapewnienia, że dane osobowe, które są nieprecyzyjne w świetle celów ich przetwarzania, zostaną niezwłocznie usunięte lub poprawione. W tym celu Spółka zapewnia, w ramach swoich wewnętrznych procedur, realizację tej zasady, w tym w szczególności zarządzanie danymi wykorzystywanymi w toku prowadzonej działalności, co obejmuje np. zarządzanie architekturą i jakością danych, z uwzględnieniem okresowej oceny jakości danych, czyszczenie danych, identyfikację przyczyn błędów występujących w danych oraz bieżące monitorowanie jakości danych.

16.2.1.5. Zasada ograniczenia przechowywania

Spółka zapewnia realizację zasady, o której mowa w art. 5 ust. 1 lit. e RODO, zgodnie z którą dane powinny być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, nie dłużej niż jest to niezbędne do celów, w których dane są przetwarzane. W tym celu Spółka, w ramach swoich wewnętrznych procedur, zapewnia realizację tej zasady i dba o to, aby skuteczność i prawidłowość kontroli w tym zakresie uwzględniała w szczególności role i zadania Inspektora Ochrony Danych.

16.2.1.6. Zasada integralności i poufności

Spółka zapewnia integralność i poufność danych w rozumieniu art. 5 ust. 1 lit. f RODO poprzez zapewnienie bezpieczeństwa danych osobowych, w tym ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem za pomocą odpowiednich środków technicznych i organizacyjnych.

16.2.1.7. Zasada rozliczalności

Spółka zapewnia realizację zasady rozliczalności, o której mowa w art. 5 ust. 2 RODO, poprzez wprowadzenie odpowiednich procedur i polityk wykazujących zgodność z przepisami RODO, ze szczególnym uwzględnieniem udziału Inspektora Ochrony Danych w tych działaniach.

16.2.2. Co zapewniamy

W celu skutecznego wdrożenia wymogów RODO Spółka zapewnia:

a. środki techniczne i rozwiązania organizacyjne odpowiednie do zagrożeń i kategorii danych, które mają być chronione;
b. szkolenia z zakresu przetwarzania danych osobowych i sposobów ich ochrony;
c. kontrola i nadzór nad przetwarzaniem danych osobowych;
d. monitorowanie podjętych środków ochrony.

16.2.3. Podstawy prawne przetwarzania danych

Spółka przetwarza dane osobowe, jeżeli spełniony jest co najmniej jeden z poniższych warunków:

a. osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
b. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
c. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Spółce;
d. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
e. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach oficjalnych uprawnień przysługujących Spółce;
f. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Spółkę lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych

interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy taka osobą jest dzieckiem.

16.3. Prawa osób, których dane dotyczą

Spółka realizuje prawa osób, których dane dotyczą, w tym:

a. prawo do informacji (obowiązek informowania);
b. prawo dostępu do danych lub otrzymania kopii danych;
c. prawo do sprostowania danych;
d. prawo do usunięcia danych;
e. prawo do ograniczenia przetwarzania;
f. prawo do przenoszenia danych;
g. prawo do sprzeciwu wobec przetwarzania.

16.4. Obowiązek informacyjny

W przypadku zbierania danych osobowych, a także zmiany celów przetwarzania danych osobowych w stosunku do celu, dla którego dane osobowe zostały zebrane, Spółka wywiązuje się z obowiązku informacyjnego.

16.5. Ocena wpływu na ochronę danych

Spółka ocenia wpływ planowanych operacji przetwarzania na ochronę danych osobowych, w przypadku, gdy zgodnie z analizą ryzyka prawdopodobieństwo naruszenia praw i wolności osób jest wysokie.

16.6. Środki bezpieczeństwa

Spółka stosuje środki bezpieczeństwa ustanowione poprzez analizy ryzyka i analizy adekwatności środków bezpieczeństwa oraz oceny wpływu na ochronę danych.

16.7. Zgłaszanie naruszeń

16.7.1. Naruszenie ochrony danych

Za naruszenie ochrony danych osobowych w Spółce uznaje się zdarzenie występujące w ramach ryzyka operacyjnego, przez które należy rozumieć możliwość wystąpienia szkody wynikającej z nieodpowiednich lub zawodnych procedur wewnętrznych, ludzi i systemów lub ze zdarzeń zewnętrznych.

16.7.2. Naruszenie ochrony danych osobowych

Naruszenie ochrony danych osobowych to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego

dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych w ramach działalności Administratora.

16.7.3. Powiadomienie o naruszeniu ochrony danych osobowych

Naruszenie ochrony danych osobowych, które podlega zgłoszeniu:

a. organowi nadzorczemu - uznaje się za sytuację, w której prawdopodobieństwo wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych zostało oszacowane przez Spółkę jako wyższe niż niskie;
b. osobie, której dane dotyczą - uznaje się za sytuację, w której Spółka oceniła ryzyko naruszenia praw i wolności osoby, której dane dotyczą, jako wysokie.

16.7.4. Sytuacje zidentyfikowane jako ryzyko naruszenia

W szczególności następujące sytuacje mogą prowadzić do naruszenia:

a. utrata danych osobowych uniemożliwiająca wykonanie zobowiązania;
b. naruszenie integralności danych osobowych z ryzykiem nienależytego wykonania obowiązku;
c. utrata poufności danych osobowych,

które mogą wystąpić w wyniku:

a. uszkodzonego lub nieprawidłowo działającego systemu informatycznego;
b. incydentów losowych lub środowiskowych;
c. niepożądanego (sabotaż/dezorganizacja) działania osób, w tym osób trzecich (kradzież, zniszczenie, uniemożliwienie dostępu, modyfikacja, ujawnienie danych);
d. błędu ludzkiego, w tym w ramach niewłaściwego postępowania personelu przy zabezpieczaniu danych osobowych.

16.7.5. Ocena ryzyka naruszenia

Z zastrzeżeniem oceny ryzyka naruszenia, podlegającym zgłoszeniu naruszeniu ochrony danych osobowych osobie, której dane dotyczą, może być w szczególności: wyciek (tj. niekontrolowane ujawnienie) informacji z bazy danych (naruszeniem podlegającym zgłoszeniu nie będzie wyciek pliku zawierającego wyłącznie nazwy ulic wraz z numerami, kody pocztowe lub nazwy miejscowości), przesyłanie dokumentów zawierających dane stanowiące tajemnicę prawnie chronioną pocztą elektroniczną/tradycyjną do osoby nieuprawnionej, przechwycenie i wyciek danych/narzędzi służących do logowania i identyfikacji osób fizycznych, utrata/kradzież dokumentów zawierających dane osób fizycznych, zerwanie plomb umieszczonych na nośnikach służących do archiwizacji dokumentów, generowanie i wykorzystywanie błędnej bazy danych do przesyłania chronionych informacji

do osób fizycznych, wysyłanie wiadomości e-mail do nieuprawnionych odbiorców, informacji uzyskanych w drodze dostępu do danych osobowych przez osobę nieuprawnioną.

16.7.6. Naruszenie ochrony danych osobowych niepodlegające zgłoszeniu

Za naruszenie ochrony danych osobowych niepodlegające zgłoszeniu organowi nadzorczemu można uznać w szczególności: wyciek (tj. niekontrolowane ujawnienie) informacji z bazy danych, które nie pozwalają na identyfikację konkretnej osoby, utratę nośnika danych z zaszyfrowanym plikiem, przy czym klucz użyty do odszyfrowania tych danych nie został złamany w wyniku naruszenia.

16.7.7. Obowiązek zgłoszenia

Obowiązek zgłoszenia powinien zostać spełniony bez zbędnej zwłoki – w miarę możliwości nie później niż w ciągu 72 godzin od wykrycia naruszenia. Naruszenie uznaje się za stwierdzone, gdy Spółka, po niezwłocznym zakończeniu postępowania wyjaśniającego zgodnie z wewnętrznymi procedurami, uzna, że prawdopodobieństwo wystąpienia ryzyka naruszenia praw i wolności jednostki zostało ocenione jako wyższe niż niskie. To, czy zgłoszenia dokonano bez zbędnej zwłoki, ustala się biorąc pod uwagę w szczególności potrzebę ustalenia przyczyn i skutków naruszenia oraz zminimalizowania tych skutków, charakter i wagę naruszenia ochrony danych osobowych, jego konsekwencje i negatywne skutki dla osoby, której dane dotyczą. Jeśli powyższy termin nie zostanie dotrzymany, powiadomieniu musi towarzyszyć wyjaśnienie przyczyny opóźnienia.

16.7.8. Ocena ryzyka naruszenia

W przypadku gdy naruszenie ochrony danych osobowych skutkowałoby wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, o naruszeniu należy niezwłocznie powiadomić osoby, których dane dotyczą, a jeżeli takie powiadomienie wymagałoby niewspółmiernie dużego wysiłku, należy wydać publiczne zawiadomienie o naruszeniu.

16.7.9. Powiadomienie osoby fizycznej

Zawiadomienie osoby fizycznej nie jest konieczne, jeżeli wdrożono odpowiednie środki ochrony obejmujące dane osobowe, których dotyczy naruszenie, i podjęto działania w celu wyeliminowania prawdopodobieństwa wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą.

16.7.10. Dokumentacja

Każde naruszenie bezpieczeństwa danych osobowych jest dokumentowane, opisując w szczególności:

a. okoliczności naruszenia, na przykład:
   - datę i godzinę wykrycia naruszenia ochrony danych osobowych;
   - opis naruszenia;
   - przyczynę naruszenia,
b. rzeczywiste i prawdopodobne konsekwencje naruszenia;
c. podjęte środki zaradcze.

16.8. Powierzenie przetwarzania danych – umowy z dostawcami

16.8.1. Wystarczające gwarancje

Spółka, powierzając przetwarzanie danych osobowych, korzysta z takich dostawców, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, tak aby przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Administratorzy, wybierając podmiot przetwarzający dane, zwracają uwagę na stosowane przez niego standardy bezpieczeństwa lub ustalają standardy, których wymagają (np. poprzez audyty lub inne formy weryfikacji).

16.8.2. Podstawa prawna

Powierzenie przetwarzania odbywa się na podstawie umowy lub innego instrumentu prawnego podlegającego prawu Unii Europejskiej lub prawu państwa członkowskiego, a zasady, na jakich odbywa się powierzenie, spełniają wymogi art. 28 RODO.

16.9. Eksport danych

Spółka stosuje politykę weryfikacji w przypadku transgranicznego przetwarzania danych oraz politykę określania wiodącego organu nadzorczego i jednostki biznesowej w rozumieniu RODO.

Poziom ochrony danych osobowych poza Europejskim Obszarem Gospodarczym (EOG) może różnić się od tego przewidzianego przez prawo europejskie. Mając to na uwadze, Spółka przekazuje dane osobowe poza EOG tylko wtedy, gdy jest to konieczne. W przypadku takiego przekazania Spółka zapewni odpowiedni stopień ochrony danych osobowych poprzez:

a. przekazywanie danych osobowych do krajów, w odniesieniu do których została wydana decyzja Komisji Europejskiej uznająca dany kraj za zapewniający odpowiedni poziom ochrony danych osobowych;
b. stosowanie standardowych klauzul umownych wydanych przez Komisję Europejską;
c. stosowanie innych odpowiednich zabezpieczeń.

17. Polityka AI

17.1. Integracja AI w Trans.eu

Trans.eu wykorzystuje sztuczną inteligencję (AI) jako kluczowy element w rozwoju i ulepszaniu swojej platformy logistycznej. Narzędzia oparte na AI służą do optymalizacji istniejących funkcjonalności, tworzenia nowych rozwiązań, automatyzacji procesów wewnętrznych oraz budowy dedykowanych narzędzi IT wspierających efektywność operacyjną. Innowacje napędzane przez AI pomagają w podejmowaniu lepszych decyzji, usprawnianiu procesów oraz poprawie doświadczeń klientów.

17.2. Zgodność i odpowiedzialne wykorzystanie AI

Mając świadomość zarówno potencjału, jak i wyzwań związanych ze sztuczną inteligencją, Trans.eu dba o to, aby wszystkie narzędzia AI – zarówno te wykorzystywane i tworzone wewnętrznie, jak i zewnętrzne – były zgodne z obowiązującymi przepisami prawa, w tym:

- **AI Act** Unii Europejskiej, który zapewnia zgodność systemów AI z zasadami przejrzystości, odpowiedzialności i etyki - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji).
- **Ogólnym Rozporządzeniem o Ochronie Danych Osobowych (RODO)**, gwarantującym, że przetwarzanie danych przez AI spełnia najwyższe standardy ochrony prywatności i bezpieczeństwa - 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 (ogólne rozporządzenie o ochronie danych).

Każdy wdrażany system AI jest poddawany szczegółowej ocenie zgodności z powyższymi regulacjami, a regularne audyty weryfikują bezpieczeństwo, rzetelność i bezstronność stosowanych algorytmów.

17.3. Etyczna AI i przejrzystość

Trans.eu kładzie nacisk na odpowiedzialne i etyczne wykorzystywanie sztucznej inteligencji, kierując się następującymi zasadami:

- **Przejrzystość** – Klienci i użytkownicy są informowani o interakcjach z funkcjonalnościami opartymi na AI oraz o roli, jaką AI odgrywa w podejmowaniu decyzji, jeśli odgrywa.
- **Odpowiedzialność** – Modele AI są monitorowane i oceniane pod kątem ryzyka błędnych decyzji, dyskryminacji lub niezamierzonych konsekwencji.

- **Integralność danych i bezpieczeństwo** – Algorytmy AI są projektowane w sposób gwarantujący poufność oraz ochronę przetwarzanych danych.
- **Nadzór ludzki** – Decyzje podejmowane przez AI, które mogłyby znacząco wpływać na użytkowników, będą poddawane weryfikacji przez człowieka w celu zapobiegania błędom i zapewnienia sprawiedliwości.

Dzięki odpowiedzialnemu podejściu do AI Trans.eu dąży do innowacji przy jednoczesnym zapewnieniu zgodności z przepisami, budowania zaufania i przejrzystości dla użytkowników.

17.4. Ocena ryzyka i minimalizacja zagrożeń związanych z AI

Aby zapewnić bezpieczne i skuteczne wdrożenie AI, Trans.eu stosuje system oceny ryzyka AI, który analizuje narzędzia i funkcjonalności AI pod kątem różnych zagrożeń:

17.4.1. Kryteria oceny ryzyka AI

Każdy system AI jest oceniany pod względem:

- **Ryzyka zgodności** – Zapewnienie przestrzegania przepisów AI Act, RODO oraz innych obowiązujących regulacji.
- **Ryzyka stronniczości i sprawiedliwości** – Weryfikacja modeli pod kątem potencjalnych uprzedzeń mogących prowadzić do niesprawiedliwych decyzji.
- **Ryzyka bezpieczeństwa** – Ocena podatności na ataki, wycieki danych i nieautoryzowany dostęp.
- **Ryzyka prywatności danych** – Weryfikacja zgodności z przepisami dotyczącymi ochrony danych osobowych.
- **Ryzyka operacyjnego** – Zapewnienie niezawodności, interpretowalności i dokładności systemów AI, aby zapobiec błędnym lub niejasnym wynikom.

17.4.2. Strategie minimalizacji ryzyka

Aby skutecznie zarządzać ryzykiem, Trans.eu wdraża następujące **mechanizmy nadzoru nad AI**:

- **Testowanie i walidacja modeli AI** – Każdy model AI przechodzi rygorystyczne testy w kontrolowanych środowiskach przed wdrożeniem.
- **Wykrywanie i eliminacja uprzedzeń** – Regularne audyty pozwalają identyfikować i korygować potencjalne uprzedzenia w algorytmach.
- **Wyjaśnialność i interpretowalność** – Modele AI zapewniają jasne uzasadnienie swoich rekomendacji.
- **Reagowanie na incydenty i monitoring** – Procesy AI są stale monitorowane, aby wykrywać nieprawidłowości i reagować na nie w czasie rzeczywistym.
- **Etyczne AI** – Wewnętrzny zespół ocenia aplikacje AI pod kątem ich zgodności z zasadami etyki.

17.5. Narzędzia AI dla klientów

Trans.eu wdraża rozwiązania oparte na AI, które zwiększają efektywność operacyjną i poprawiają doświadczenia użytkowników. Chatbot AI wspiera obsługę klienta poprzez natychmiastową obsługę zapytań – automatyczne odpowiedzi na najczęstsze pytania użytkowników.

17.6. Ciągłe doskonalenie i przyszłość

Trans.eu stale rozwija swoje systemy AI poprzez:
- Uwzględnianie opinii użytkowników, aby lepiej dopasować rekomendacje AI.
- Regularne aktualizacje modeli AI, aby odzwierciedlały zmieniające się realia branży.
- Współpracę z instytucjami badawczymi i ekspertami, aby wspierać innowacje w logistyce.

Dzięki przejrzystemu, etycznemu i zgodnemu z regulacjami podejściu, Trans.eu zapewnia, że AI pozostaje narzędziem wspierającym, a nie zagrożeniem.

18. Bezpieczeństwo eCMR w ramach Platformy Trans.eu

18.1. Charakterystyka rozwiązania eCMR

Moduł eCMR stanowi integralną część Platformy Trans.eu i korzysta ze wspólnej infrastruktury oraz środków bezpieczeństwa opisanych w niniejszym dokumencie.

Celem rozwiązania eCMR jest zapewnienie w pełni cyfrowego, bezpiecznego oraz zgodnego z przepisami prawa obiegu elektronicznego dokumentu przewozowego CMR.

Rozwiązanie eCMR jest zgodne z następującymi aktami prawnymi:
- Protokołem dodatkowym do Konwencji CMR,
- Rozporządzeniem eIDAS w zakresie stosowania kwalifikowanych podpisów elektronicznych,
- Rozporządzeniem eFTI (European Freight Transport Information).

Trans.eu wykorzystuje technologię IBM Hyperledger Blockchain, zapewniającą trwały i niezmienny rejestr danych.

18.2. Model autoryzacji i zarządzania uprawnieniami

Moduł eCMR wykorzystuje wspólny proces autoryzacji użytkowników Platformy Trans.eu, obejmujący m.in. uwierzytelnianie dwuskładnikowe ((2FA - two-factor

authentication), przelew weryfikacyjny na kwotę 1 PLN oraz walidację danych przedsiębiorstwa (KRS, NIP).

W ramach rozwiązania eCMR zdefiniowane są role użytkowników:
- Administrator,
- Manager,
- Pracownik,
- Płatnik (zgodnie z Regulaminem eCMR).

System umożliwia obsługę wielu oddziałów w ramach jednej organizacji, z zapewnieniem pełnej separacji danych oraz kontrolowanej widoczności dokumentów.

18.3. Widoczność i dostępność dokumentów

Każdy dokument eCMR posiada unikalny identyfikator oraz kompletną historię wszystkich operacji. Zakres widoczności dokumentu pomiędzy uczestnikami procesu przewozowego (nadawca, przewoźnik, odbiorca) uzależniony jest od etapu realizacji przewozu. Dostęp do dokumentu jest automatycznie ograniczany po jego zakończeniu.

Wszystkie działania użytkowników, w tym podpisy, akceptacje, edycje, eksporty PDF oraz wydruki, są rejestrowane w logach systemowych oraz w rejestrze blockchain.

18.4. Podpis elektroniczny i potwierdzenie dostawy

Podpisy składane w systemie eCMR są możliwe wyłącznie z poziomu autoryzowanych kont użytkowników Platformy Trans.eu.

W przypadku operacji realizowanych poza systemem (np. potwierdzenie wydania towaru w miejscu rozładunku) stosowany jest mechanizm dwóch unikalnych kodów autoryzacyjnych (SMS/e-mail), przypisanych do nadawcy i odbiorcy. Tylko osoba dysponująca prawidłową parą kodów ma możliwość potwierdzenia odbioru towaru.

W celu umożliwienia udziału w procesie podmiotom niezarejestrowanym na Platformie Trans.eu, moduł eCMR wykorzystuje bezpieczny mechanizm autoryzacji z wykorzystaniem kodów SMS lub wiadomości e-mail. Umożliwia on partnerom zewnętrznym potwierdzanie czynności załadunku lub rozładunku bez konieczności posiadania konta, przy zachowaniu pełnej rozliczalności działań.

Proces ten polega na przesłaniu unikalnych kodów przypisanych do dokumentu eCMR do osób kontaktowych wskazanych dla danego partnera, a ich wprowadzenie przez przewoźnika skutkuje automatycznym zarejestrowaniem podpisu w odpowiedniej rubryce dokumentu.

Planowane jest rozszerzenie tej funkcjonalności o możliwość pełnej identyfikacji użytkownika w rubrykach dokumentu oraz w historii operacji.

18.5. Bezpieczeństwo i zgodność techniczna

Rozwiązanie eCMR funkcjonuje w ramach infrastruktury Platformy Trans.eu hostowanej w centrach danych Talex (Polska) oraz AWS (Luksemburg). Dane użytkowników są przetwarzane w obszarze Unii Europejskiej.

Wszystkie dane są szyfrowane zarówno podczas transmisji (protokół TLS), jak i w spoczynku (standard AES), zgodnie z zasadami opisanymi w Sekcji 8. Szyfrowanie danych.

Moduł eCMR objęty jest regularnymi testami bezpieczeństwa i testami penetracyjnymi, zgodnie z zasadami opisanymi w Sekcji 2.3. Zakres audytów.

Każdy dokument eCMR w formacie PDF posiada unikalny identyfikator umożliwiający jednoznaczną weryfikację jego pochodzenia.

18.6. Interfejsy i integracje

Moduł eCMR udostępnia interfejs API umożliwiający integrację z systemami zewnętrznymi, takimi jak WMS lub TMS.

Dodatkowo dostępna jest funkcjonalność „Smart importer", pozwalająca na import danych z plików w formatach CSV lub XLS.

W sytuacjach wyjątkowych możliwe jest również uzyskanie dokumentu w wersji papierowej, zgodnie z art. 4 Protokołu dodatkowego do Konwencji CMR.

18.7. Zarządzanie incydentami bezpieczeństwa

Incydenty dotyczące modułu eCMR są obsługiwane zgodnie z procedurami opisanymi w Sekcji 12. Zarządzanie incydentami.

Zgłoszenia analizowane są przez Zespół Bezpieczeństwa Trans.eu, a w przypadkach wymagających interwencji prawnej – również przez Zespół Prawny i Inspektora Ochrony Danych (IOD).