Security Whitepaper

Information Security, Personal Data Privacy, Cybersecurity, AI Aspects

As at the date of 18th of March 2026

This document is disclosed publicly

Trans.eu Group S. A.

with its registered office in Wrocław, at ul. Racławicka 2-4, 53-146 Wrocław, Poland, entered into the Register of Entrepreneurs of the National Court Register by the District Court for Wrocław-Fabryczna in Wrocław, VI Commercial Division of the National Court Register under KRS number: 0000720763, NIP (tax identification number): 8942764658, REGON: 932920615, share capital: 203.500,00 PLN paid in full

Document versions table

Ver. No.	Introduction date	Document name	Introduced changes
1.0	7 Nov 2023	Security Whitepaper	None - this is the first version of the document.
1.1	8 Nov 2023	Security Whitepaper	Section 6.1:application name “Loads2DO” changed to “Loads4Driver”
1.2	30 Aug 2024	Security Whitepaper	1. Updated ISO 27001 certificate information 2. Added Section “Users authorization” 3. Updated section numbering and table of contents
1.3	5 Mar 2025	Security Whitepaper	1. Updated Section “Data centers - Overall hosting architecture” 2. Updated Section “Data transmission” 3. Updated Section “High availability” 4.. Added Section “AI Policy” 5. Corrected page numeration
1.4	11 Aug 2025	Security Whitepaper	1. Updated ISO 27001 certificate information 2. Updated share capital
1.5	1 Nov 2025	Security Whitepaper	1. Added Section “Security measures for eCMR in the Trans.eu Platform” 2. Updated table of contents
1.6	18 Mar 2026	Security Whitepaper	1. Updated authentication verification methods

Introduction

Trans.eu Group S.A. (**"Trans.eu"**) delivers a scalable logistics platform that brings together shipping companies, logistics operators, forwarders and carriers. It is designed for high availability and dependability, providing the tools that enable customers to run a wide range of tasks empowering their business processes.

This document is intended to provide an overview of an Trans.eu core infrastructure design, including its approach to security, personal data protection and high availability. To make it easier to comprehend, it is divided into sections listed in the Table of content.

In Trans.eu we believe that security is not a state but a continuous pursuit of everbetter solutions aimed at protection of what is of value - especially including precious data of our customers. Therefore we often implement new security solutions and need to update this document. If whatever information collected within this document does not satisfy your need for knowledge and/or you have any doubts, please, do not hesitate to contact us - we will do our best to ease all your security worries and concerns.

Table of contents

Document versions table **2**
Introduction **3**
Table of contents **4**
1. Data Security Management **7**
1.1. ISO 27001 Certification 7
1.2. Technical, organizational and legal security means 8
1.3. Policies and procedures 8
2. Security audits **8**
2.1. Internal and external audits 8
2.2. Automatic and traditional audit methods 9
2.3. Audit scopes 9
2.4. Audit frequency 9
3. Overall system and system access security solutions **10**
3.1. General 10
3.2. Data centers - Overall hosting architecture 10
3.3. Data transmission 12
3.4. High availability 12
3.5. Data backups and configuration safe-guards 13
3.6. Infrastructure management 14
3.7. In-house and external users management 14
4. Network security **14**
4.1. General 14
4.2. Internet connection 15
4.3. Logging, monitoring and incident management 15
5. Physical access control **15**
5.1. Data centers physical access control 15
5.2. Organisation’s premises access control 16
6. Customer access **16**
6.1. Trans.eu Platform Access 16
6.2. Users authorization 16
6.3. Customer multi-factor authentication (MFA) 17
6.4. User account management and user account type (role) 17
7. Personnel access **17**
7.1. On-boarding and off-boarding procedures 17
7.2. Personnel access scope 17
7.3. Personnel access standards 18

7.4. VPN protected remote work 18
7.5. Personnel multi-factor authentication (MFA) 18
8. Data encryption 18
8.1. High encryption standards 18
8.2. In transit encryption 19
8.3. At rest encryption 19
9. Change and patch management 19
9.1. Change management 19
9.2. Patch management 20
10. Backups 20
10.1. Frequency 20
10.2. Location 20
10.3. Maintenance 20
11. Servers 20
11.1. Support 20
11.2. Updates and patches 20
12. Event and incident management 21
12.1. Event management 21
12.2. Incident management 21
12.3. Event and incident categories 21
13. Personnel security training 21
13.1. Onboarding training 21
13.2. Renewed training 22
14. Third party security management 22
14.1. Subcontractors and vendors homologation process and risk assessment 22
14.2. Client security management homologation process and risk assessment 22
15. Business Continuity and Disaster Recovery 22
15.1. Backups 22
15.2. Business Continuity 23
15.3. Disaster Recovery 23
16. Personal data security 23
16.1. Compliance with the GDPR 23
16.2. Principles for personal data processing, legal grounds for processing 24
16.2.1. Principles for personal data processing 24
16.2.1.1. Lawfulness, fairness and transparency principle 24
16.2.1.2. Purpose limitation principle 24
16.2.1.3. Data minimisation principle 25
16.2.1.4. Accuracy principle 25
16.2.1.5. Storage limitation principle 25
16.2.1.6. Integrity and confidentiality principle 26

16.2.1.7. Accountability principle 26
16.2.2. Our Assurances 26
16.2.3. Legal grounds for data processing 26
16.3. Data subject rights 27
16.4. Obligation to inform 27
16.5. Data protection impact assessment 27
16.7. Reporting of violations 27
16.7.1. Data breach 27
16.7.2. Personal data breach 28
16.7.3. Personal data breach notification 28
16.7.4. Situations identified as breach risk 28
16.7.5. Subject to the assessment of the risk of a breach 28
16.7.6. Not notifiable personal data breach 29
16.7.7. Notification obligation 29
16.7.8. Risk assessment of a breach 29
16.7.9. Notifying an individual 29
16.7.10. Documentation 30
16.8. Entrustment of processing - supplier agreements 30
16.8.1. Sufficient guarantees 30
16.8.2. Legal basis 30
16.9. Data export 30
17. AI Policy 31
17.1. AI Integration in Trans.eu 31
17.2. Compliance and responsible AI use 31
17.3. Ethical AI and transparency 31
17.4. AI Risk assessment and mitigation 32
17.4.1. AI risk evaluation criteria 32
17.4.2. Risk mitigation strategies 32
17.5. AI-powered customer-facing tools 33
17.6. Continuous Improvement & Future AI Development 33
18. Security measures for eCMR in the Trans.eu Platform 33
18.1. Characteristics of the eCMR solution 33
18.2. Authorization and access control model 33
18.3. Document visibility and accessibility 34
18.4. Electronic signature and delivery confirmation 34
18.5. Technical security and compliance 35
18.6. Interfaces and integrations 35
18.7. Security incident management 35

1. Data Security Management

1.1. ISO 27001 Certification

Since 2016, Trans.eu has had an Information Security Management System implemented compliant with the ISO/IEC 27001 standard. The system is regularly audited and is granted the appropriate certification. The high standard of the conducted audits is backed by the reputation of the certifying auditor - Dekra Certification Sp. z o.o. which is accredited by PCA (Polskie Centrum Akredytacyjne - the national accreditation body of the Republic of Poland) and is a member of IAF (International Accreditation Forum, Inc. - a multilateral recognition arrangement).

You may find the current certificate here: ISO 27001 Certificate.

Trans.eu stays up to date with the evolution of ISO 27001 norm. Below you can find the list of ISO 27001 certificates acquired by Trans.eu.

Table 1. ISO 27001 certificates history

Period	ISO 27001 norm version	Scope of certification	Accreditation body
2016-2019	ISO/IEC 27001:2013	Providing IT solutions for branches: transportation, shipping and logistics	Dekra Certification GmbH
2019-2022	ISO/IEC 27001:2017	Providing IT solutions for branches: transportation, shipping and logistics	Dekra Certification GmbH
2022-2024	ISO/IEC 27001:2017	Providing IT solutions for branches: transportation, shipping and logistics	Dekra Certification GmbH
2024-2025	ISO/IEC 27001:2017	Providing IT solutions for branches: transportation, shipping and logistics	Dekra Certification Sp. z o.o.
2025-2028	ISO/IEC 27001:2022	Providing IT solutions for branches: transportation, shipping and logistics (planned)	Dekra Certification Sp. z o.o.

To get the ISO 27001 certificate a company needs to undergo a thorough audit of the Information Security Management System. The ISO 27001 certificate is issued for 3 years but to maintain the certificate the company needs to undergo control audits of the ISMS after each year.

1.2. Technical, organizational and legal security means

To ensure information security, data privacy and cybersecurity Trans.eu introduced and maintains numerous technical, organizational and legal security means most of which are described in this document.

1.3. Policies and procedures

Trans.eu maintains an information security policy applicable to all of its personnel. This information security policy is periodically reviewed, approved, communicated to all employees and is inline with industry recommended standards. Trans.eu also has a formal information risk management process in place that prioritizes, documents and tracks identified risks to closure. Internal audits are regularly performed to ensure Trans.eu's compliance with its information security policies and guidelines. Trans.eu also has a privacy policy in place that governs the protection of personal data including customer personal information (personal data protection is further described in Section 16. Personal data security).

There is a formal data classification schema that applies to customer data that defines the level of protection depending on the classification (e.g. public, internal, confidential, etc.). Trans.eu has defined processes and technology to segregate customers' data to ensure integrity and confidentiality. There are also documented and approved processes and procedures for encryption key management (e.g. PKI, certificate authority, key distribution, and rotation).

Trans.eu maintains an up-to-date and complete inventory on hardware, virtual machines, software and applications.

2. Security audits

2.1. Internal and external audits

Trans.eu constantly undergoes security audits. Internal audits are carried out at least on an annual basis to measure compliance, effectiveness and security (e.g. application security scans and audits, internal ISO 27001 compliance audits). Internal ISO 27001 compliance audits are carried out by certified internal auditors. External audits are also carried out at least once a year and always by renowned third parties that can back up the quality of the audit with their own reputation and professionalism (e.g. application, internal IT infrastructure and CRM security audits carried out by Securitum Audyty Sp. z o.o. Sp.k., ISO 27001 certification audit carried out by Dekra Certification Sp. z o.o.).

2.2. Automatic and traditional audit methods

Trans.eu always picks an adequate audit method. While most of the audits are carried out the traditional way (e.g. internal and external ISO 27001 compliance audits, manual parts of security audits carried out by Securitum Audyty Sp. z o.o. Sp.k.), wherever possible, automatic audit methods are applied to boost the frequency of the audits (e.g. automatic security scans of the application or its parts (modules)).

2.3. Audit scopes

Trans.eu frequently undergoes a variety of audits to address the ISMS, the application itself and all elements of the system. ISO 27001 compliance audits verify Trans.eu's ISMS compliance with ISO 27001 norm, i.e. how well Trans.eu manages security of information it processes. Application and IT infrastructure security audits verify applied technical security means. They include scans of the whole application and internal infrastructure environment aimed at vulnerability detection, bugs, security gaps and removal/mitigation of such vulnerabilities, bugs and security gaps. They consist (among other elements) also of penetration tests (pentests). Security audits of the application cover the whole Trans.eu Platform, including its environment, integrated applications and the products and product lines. Security audits of all elements of the system cover each of the elements separately and also include pentests of these elements.

2.4. Audit frequency

All kinds of audits (including automatic and manual scans and pentests) are carried out at least once a year, although most of them are more frequent - usually once every three to six months. To get the ISO 27001 certificate a company needs to undergo a thorough audit of the ISMS. The ISO 27001 certificate is issued for 3 years but to maintain the certificate the company needs to undergo control audits of the ISMS after each year. Application and IT infrastructure security audits frequency (especially pentests) varies from a year to 3 months. Application also undergoes a static code analysis aimed at vulnerability detection after every introduced change (always before production launch).

3. Overall system and system access security solutions

3.1. General

Trans.eu consistently applies and manages secure configurations on its systems, applications and network devices, and has mechanisms to detect and correct configuration drift.

Malware defense mechanisms are in place that are deployed on all our computing devices and are configured to perform scans and to get file definition updates from a trusted source.

All the running versions of operating systems, virtualization, networking, middleware, databases and application software in our environment are still supported by the corresponding vendor.

There are processes and tools in place to back up customer information or services, protect the backups against tampering and a proven methodology for the timely recovery of information or services.

Trans.eu uses processes and tools to track, control, prevent and correct the use, assignment and configuration of administrative privileges on computers, networks and applications.

Trans.eu uses mechanisms to segregate and protect internal networks from untrusted networks.

Trans.eu has processes for maintaining the integrity of secure configurations for hardware and software, including detecting and addressing configuration drift.

Trans.eu has a process in place to life-cycle and securely dispose of hardware used in the organization (servers, workstations, laptops, mobile phones or tablets, USB storage devices, etc.).

3.2. Data centers - Overall hosting architecture

Trans.eu is hosted within two major data centers in Europe. One of them is located in Poland and is provided by Talex (https://www.talex.pl/), partner for data center services in Central and Eastern Europe. The second one has been delivered on top of Amazon's AWS, world's most comprehensive and broadly adopted cloud platform.

Both locations selected for Trans.eu hosting are state-of-the-art data processing centers, with strong physical and logical security models, constant monitoring, activity records, CCTV and more. Design of both stands up to the best practices available.

Talex's data center complies with the requirements of Data Centre Operations Standard; DCOS-4 certification ensures high availability of the services provided by this data center and guarantees that the operator's procedures are well-defined, tested, documented, with their quality and adequacy constantly monitored and improved. The data centers possess ISO/IEC 27001 compliant ISMS.

A virtual data center maintained within Amazon's AWS cloud platform, designated for lighter but heavily scalable part of Trans.eu that handles constantly changing load and networking patterns, is a part of AWS Global Cloud Infrastructure. You can read more about it on Amazon's AWS web sites using links provided at the end of this section (Table 2).

Talex's and AWS' data centers are connected together with dedicated MPLS circuits and VPN tunnels. Also, all three data centers have dedicated, publicly available endpoints bounded logically as one, uniform entry point for Trans.eu Platform customers (separately for retail and enterprise clients). Having this, Trans.eu Platform is ready for taking most of available CDN and geo-location features, and can sustain most of the critical routing outages or blackouts in the Internet.

Table 2. Data centers

Data Center	**TALEX**	**AWS**
Service provider	**"Talex" S.A.**	**Amazon web Services EMEA SARL**
	ul. Karpia 27D 61-619 Poznan Poland, EU	38 Avenue John F. kennedy L-1855 Luxembourg Luxembourg, EU
	KRS number: 0000048779	RCS number: B186284
Services	https://www.talex.pl/en/services/collocation/	https://aws.amazon.com/compliance/data-center/data-centers/
Controls	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-infrastructur

		e/
Locations	European Union https://www.talex.pl/en/services/talex-data-center/	European Union https://aws.amazon.com/about-aws/global-infrastructure/

3.3. Data transmission

Primary component in both data centers responsible for proper communication and data security in Trans.eu is its network layer. Although network stack and data flow design for cloud environment in AWS differs from corresponding implementation in Talex's data center, both share the same strict principles regarding edge protection, control and data-plane isolation, tiers and redundancy.

In both data center locations network configurations employ granular subnetting (depending on a given subnet's designated function), network tiers (used for enforcing IP traffic direction and segmentation), both supported by proper routing and firewall policies. Both data centers use multiple ISP connections for handling high network throughput, load-balancing and redundancy.

In Talex's location separate edge, DMZ and LAN segments are maintained, each protected by redundant firewalls. Applied solutions allow increased availability of Trans.eu services. All IP traffic in Talex's data centers is being monitored directly and indirectly.

Virtual data center in AWS isolates Trans.eu components on a VPC level. Application and network load balancers stand as the first level of protection, next to built-in within AWS platform security features. Whole network traffic in AWS is being monitored.

3.4. High availability

Trans.eu has been built with high-availability in mind, starting from blueprints for both infrastructure and application, making them complementary in terms of common goals but still decoupled. With this approach software, compute, data and communication layer designs could be developed independently, allowing to run Trans.eu services in high-availability mode regardless of the data center they were scheduled to operate.

In both data-center locations multiple, yet sometimes specific for each infrastructure, technical solutions are used to achieve HA.

Both data centers use multiple ISP services for Internet access and public visibility. Interconnection links between all locations are also redundant.

All services endpoints, regardless of their location, are available via single logical query endpoint through service-discovery layer, with public endpoints being prepended on the edge tier with additional ISO/OSI layer 4 and layer 7 load balancers and furthermore – with CDN.

In Talex's location, services are available as virtual machines running on highly capable and highly available storage and hypervisor farms, spread between multiple, interconnected server racks equipped with redundant power supplies, communication devices, links, etc. Applied solutions allow for overwatching and predicting all necessary hardware upgrades and features as they deem necessary in a matter of next 3-6 months, which grants additional spare space for extra load or unpredicted hardware failure.

In AWS, where most services must face constantly changing load and networking patterns while embracing the nature of cloud computing, Trans.eu components make use of multiple availability zones, auto-scaling groups, container capacity providers and application auto-scaling. Combination of all these features allows for fast, fault tolerant scaling of multiple services at the same time according to current usage demands, without any drawback or side effect on the rest of the system. These tactics allow for employing as much prediction mechanics and automation as the selected cloud provider can deliver.

All Trans.eu components are being constantly monitored on 24/7 basis with an on-duty response team ready to act, if for some reason automatic healing and fail-over tactics will not recover malfunctioning components to meet required operational level.

All network systems and server systems employ redundancies such as redundant equipment.

3.5. Data backups and configuration safe-guards

All application components of Trans.eu services have been designed and implemented to be completely stateless. This allowed to reduce backup operations to databases and shared file systems only, which simplified scheduling process, retention policies and disaster recovery tests.

All data backups, from each data center location, are subject to cross-location and off-site storage policy, which allows Trans.eu operations task force to perform full data recovery in case of catastrophic disaster in one of our data centers.

Additionally, by having all infrastructure managed by configuration managers and infrastructure-as-code tools with the help of modern code repository solutions, Trans.eu systems can be safely re-deployed in a completely new data center, in case when use of a given location will no longer be available.

3.6. Infrastructure management

All Trans.eu infrastructure is directly managed by infrastructure-as-code solutions and configuration managers. That said, having all configuration versioned and stored within a code allowed for drastically reduced deployment time and roll-back events, along with automated validation, testing and provisioning of new services using CI/CD pipelines. It also ensured implementation of the same security protocols across all of Trans.eu components, making virtually no room for human error to occur.

3.7. In-house and external users management

Direct infrastructure access for each group of users – developers and operations task force – is maintained by both network security policies and distributed directory services. All data centers take advantage of fine-grade access control provided by integrated LDAP solutions.

Separate security policies are used for each group of users or even at a single user level, depending on a level of trust, area of responsibility and the principle of least privilege. While the operations team is usually allowed to access most, if not all components of the Trans.eu system on both control and data plane, development teams are granted only specific endpoints for read-only validation access.

Remote access to all computing and data resources, including servers, container clusters, code repositories, etc. is secured by VPN solutions with highly restrictive access policies integrated with Deep Packet Inspection (DPI) solutions. VPN access to all critical resources of Trans.eu is available only for a limited group of users (operations, on-duty response team) and is being constantly monitored.

4. Network security

4.1. General

Protection of systems against DDoS and brute force attacks is in place.

There is suitable network segmentation in place.

If remote administration is necessary, it is approached via secure communication channels. It is implemented using high encryption standards.

There is encrypted communication with subcontractors (e.g. external service providers for operation of the data centers) used. It is implemented using high encryption standards (Section 8. Data encryption).

4.2. Internet connection

There are multiple Internet connections available at each data center. There is an automatic detection of Internet connection failure in place. There is automatic activation and redirection of traffic to a secondary Internet connection in place, if the primary connection goes down (i.e. failover).

4.3. Logging, monitoring and incident management

There is 24/7 monitoring of the infrastructure (availability of services and resources). Fast internal reaction to attacks and/or other security incidents. Monitoring of logs and evaluation of data sources (system status, erroneous authentication attempts) is conducted frequently. Trans.eu has also implemented process/technology to ensure important audit logs (e.g. operating systems, networks, databases, applications, etc.) are tamper resistant.

5. Physical access control

5.1. Data centers physical access control

You can obtain detailed information on physical access control of each of the data centers referred to in Section 3.1. from these data centers - e.g. from their websites as referred to in Table 2 (Section 3.2. Data centers - Overall hosting architecture). All of the data centers (among other physical access controls) provide:

Data center location

- Video surveillance outside of the data center.
- Video surveillance inside the data center (in-doors and rack corridors).
- Monitored buildings.
- Burglar alarm systems.
- 24x7x365 security guards control access to each building.
- Front desk with required sign in for visitors.
- Walls / fences surrounding the buildings.

- Access to employee or visitor parking is restricted by barriers and/or security guards.

Data center buildings

- Buildings with no windows.
- Separate physical security zones for general areas, customer-accessible areas and data center.
- Separately locked racks with the possibility to use custom locks and keys.

Data center access

- Multi-factor security for granting access, logged.
- Management of keys and documentation of key holders.
- Electronic access card reading system.
- Physical access to data processing equipment can be performed only by authorised, security aware stuff.
- Visitors accessing buildings are always escorted.
- Access to employee or visitor parking is restricted by barrier and/or security guard.

5.2. Organisation’s premises access control

Physical controls in place to prevent unauthorized access to customer dedicated workspaces (among others):

- Access to Trans.eu’s premises is restricted.
- Access to Trans.eu’s premises is controlled via electronic keyes and traditional keyes.
- Access to Trans.eu’s office areas is protected by doors equipped with access control.
- Visitors accessing Trans.eu’s premises are always identified, logged and escorted.
- Trans.eu’s premises and their surroundings are monitored using CCTV cameras.

6. Customer access

6.1. Trans.eu Platform Access

Customers may access Tran.eu Platform through:

- Internet browser (we recommend Google Chrome) at www.platform.trans.eu;
- Android/iOS application: Loads2GO and Loads4Driver;
- API interface (see more at: https://www.trans.eu/api/).

6.2. Users authorization

Every Customer (company) applying for access to the Trans.eu Platform must be authorized. The authorization process is carried out on the basis of regularly reviewed and updated procedures and is intended to eliminate potential threats to and from the company’s future contractors, among others:

- fictitious data - the authorization process helps to check if all Customers’ information about their company and the way they carry out their business affairs is real and up to date;
- dangerous connections - the authorization process helps to ensure that a new Customer registering to the Trans.eu Platform is not connected personally or financially to a former Customer who ended up posing a threat to other Trans.eu Platform users;
- impersonation of the company - the authorization process helps to check that the people who register a company as a Customer on the Trans.eu Platform are really the people authorized to formally represent the company and that the company itself is an operating company formally registered in the country of origin.

The process of authorization also checks if the company trying to get access to the Trans.eu Platform is a company operating on the logistics market (and not a market that is not related to logistics at all).

6.3. Customer multi-factor authentication (MFA)

To access Trans.eu Platform all Customers must use at least two-factor authentication (2FA) using the factor of choice (e-mail, text message, OTP password, dedicated application).

There is also a documented password policy for users in place and effective.

6.4. User account management and user account type (role)

A company is able to manage its employees user accounts by creating and blocking Related User Accounts and choosing an appropriate type of account for several role types of employees.

7. Personnel access

7.1. On-boarding and off-boarding procedures

Trans.eu has implemented on-boarding and off-boarding procedures which cover granting and revoking access to data and information processed by Trans.eu.

7.2. Personnel access scope

The personnel gets access to data and information processed by Trans.eu in accordance with an internal set of rules which determine the scope of data and information accessible by each member of the personnel depending on their role, responsibilities, etc. These rules apply equally to the new hires and transfers. Trans.eu also has a defined policy for managing privileged account accesses.

7.3. Personnel access standards

Trans.eu complies with the following standards:

- permissions to systems and networks is restricted to only those who require access for performing their job responsibilities;
- access is disabled promptly after it is no longer needed;
- access requests are properly approved before granted;
- access reviews are conducted periodically.

The access of the personal and individual user / administrator is logged-in when entering the system and / or corporate.

There is a documented set of rules, which describes the administration process of internal user accounts. It is a set of standard and documented procedures with clearly defined roles and responsibilities for access provisioning, including new hires, transfers, and terminations for all personnel members. The access management process includes managing inactive user accounts.

There is also a documented password policy for internal users in place and effective.

7.4. VPN protected remote work

Whenever working remotely from any place outside the office the Trans.eu personnel uses VPN to securely access users'/customers' data.

7.5. Personnel multi-factor authentication (MFA)

To access Trans.eu systems and data all Trans.eu personnel must use at least two-factor authentication (2FA).

8. Data encryption

8.1. High encryption standards

Trans.eu uses high encryption standards: Advanced Encryption Standard (AES).

8.2. In transit encryption

Depending on the case, data in transit are encrypted using an adequate method:

Table 3. In transit encryption

Context	Encryption technology/method
A file attached to an email	PDF / Excel / Word / ZIP Archive etc. file or folder secured with a password
Systems and data accessed remotely for work purposes by the personnel Cloud usage	VPN
Platform access by users	TLS

8.3. At rest encryption

All back-up data and all hard drives, including mobile devices (i.e. phones, laptops) are encrypted using Advanced Encryption Standards (AES).

9. Change and patch management

9.1. Change management

Change management process is established and documented. Change requests are documented and stored, approved by an appropriate business representative, the potential business impact is evaluated. Changes are always tested to determine the expected results. Trans.eu uses separate environments (production vs.non-production) in the change management process. Changes are reviewed to ensure that they do not compromise security controls.

There is a standard, formal, and documented IT change management process in place to manage and control changes in Trans.eu’s IT environment. This process requires formal approval of all changes. It also captures a clear description of the change, impact of the change, test plan, back-out plan, planned timings for the change and status of the change.

9.2. Patch management

Trans.eu has implemented a secure software development process. There are policies and procedures in place that prevent use of client's production data in non-production environments, such as Trans.eu’s employee desktop systems or systems used for development, testing, or QA. Trans.eu also has a process to monitor and apply software patches on systems and applications. Patch management process is established and documented. Patches are always tested to determine the expected results.

10. Backups

10.1. Frequency

Data backups are conducted frequently to secure clients’ and Trans.eu’s data considering the dynamic nature of the Trans.eu Platform.

10.2. Location

Data backups are stored offline and separately from the servers’ locations.

10.3. Maintenance

The backup process includes periodic data restoration and testing to ensure availability and integrity of data covered by the backup. Trans.eu has a process to monitor and recover from backup failures.

11. Servers

11.1. Support

There are support agreements in place for appropriate 3rd party software and hardware used within the server infrastructure.

11.2. Updates and patches

Critical new software updates and patches released by software/hardware providers are installed on our Trans.eu's servers shortly after release. Software updates and patches are first tested in a separated environment before servers are updated or patched.

12. Event and incident management

12.1. Event management

There is regular event monitoring established and frequent reviews are performed. All appropriate event types (e.g. system crash, object deletion, failed password) are recorded and stored for a set period of time.

12.2. Incident management

Security incident management process is established and documented. Trans.eu has a formal incident and problem management strategy that includes communication and escalation procedures. Also Trans.eu tracks and monitors information security events to ensure they are reviewed, prioritized, assigned and remedied in a timely manner.

12.3. Event and incident categories

Events that are recognised as a security threat may be qualified as:

- an event which is not an incident, i.e. does not breach security of any data and/or information;
- a cybersecurity incident, i.e. an event covering security breach of the IT systems;
- a GDPR incident, i.e. an event covering security breach of personal data;
- an ISO incident, i.e. an event covering security breach of data and/or information.

An event may constitute none, one, two or all of the abovementioned types of incidents. Therefore events are analyzed in various aspects to ensure all potential security dimensions are verified and reaction to the event is thorough.

Some events do not become incidents but reveal a potential threat (e.g. vulnerabilities, bugs, etc.) and are addressed properly.

Incident’s impact on security is rated on a four-level scale: low, medium, high and critical and is taken care of adequately.

13. Personnel security training

13.1. Onboarding training

The onboarding process of the new personnel members includes security training covering information security and personal data protection.

13.2. Renewed training

Security training can be renewed on an internal e-learning platform. Security rules are also reminded during various internal audits and whenever they are improved.

14. Third party security management

14.1. Subcontractors and vendors homologation process and risk assessment

Our subcontractors and vendors undergo a homologation process and risk assessment to ensure that they comply with legal and security requirements adequate to data and information they might have access to. The homologation process and risk assessment take place before concluding an agreement with a given subcontractor and/or vendor and are regularly redone during the course of the agreement.

14.2. Client security management homologation process and risk assessment

To ensure safety regarding business relations and transactions our clients need to undergo the verification and authorisation processes described in the Regulations of the Trans.eu Platform (available at: https://www.trans.eu/en/regulations/). The authorisation process is carried out in accordance with internal authorisation procedures (part of strictly confidential internal security documentation). Without authorisation a client does not have access to the Trans.eu Platform. Whenever necessary (e.g. Regulations of the Trans.eu Platform infringement) a client may be obliged to undergo the authorisation process again (i.e. reauthorisation process).

These processes allow Trans.eu to give access to the Trans.eu Platform not just to anyone but only to verified companies. The processes are fraud-minimization means (among other means). Trans.eu creates a more and more safe environment for Trans.eu Platform users.

15. Business Continuity and Disaster Recovery

15.1. Backups

All Trans.eu Platform data and other data processed in Trans.eu internal infrastructure is backed up and encrypted (Section 8. Data encryption) to a separate server in a physically separate data center. Backups are conducted frequently.

The backup policy covers:

- all production systems;
- all test, stage and development instances;
- all other data.

Backups are stored in secure, encrypted form on a secure, durable, storage service. The selected backup location is always different from the location of the production server.

The backups are constantly monitored by comparing versions to ensure they are of similar size. This allows us to quickly identify any problems with backups.

15.2. Business Continuity

Trans.eu has multiple offices in several locations in the EU, with the principal ones located in two separate locations in Wrocław, Poland. No critical data infrastructure exists at any of these offices. Trans.eu is fully capable of normal operations even if any of these offices are affected by a disaster. All operations can be continued by Trans.eu personnel remotely.

15.3. Disaster Recovery

Damage to the hardware of any instance of Trans.eu can be remedied within an appropriate amount of time.

Recovery time objective (RTO)
The RTO is to have Trans.eu Platform back up and running within an appropriate amount of time after a major catastrophe regarding the server facility, or quicker if only the server hardware itself was damaged.

Recovery point objective (RPO)
The RPO is set to be appropriately recent status of data.

16. Personal data security

16.1. Compliance with the GDPR

Protecting the personal data of our customers and employees is a priority for Trans.eu.

In this regard, our Company makes every possible effort to meet the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC – General Data Protection Regulation, (hereinafter: the GDPR).

Our ongoing compliance efforts build on existing investments in protecting privacy, confidentiality, ensuring security and implementing the operating procedures necessary to comply with the GDPR and other applicable regulations. Trans.eu, acting both as Controller and data processor, understands the obligations that follow in complying with the GDPR.

If you would like to know the details and principles of Trans.eu's processing of your personal data, READ **OUR PRIVACY POLICY**, available at: https://www.trans.eu/en/privacy-policy/ and **the Trans.eu Platform Terms and Conditions**, available at: https://www.trans.eu/en/regulations/.

Moreover, if you would like to know about cookies, you can find detailed information on the Trans.eu's use of cookies is set out in the **Cookie Policy** available on the website: https://www.trans.eu/en/cookie-policy-eu/.

16.2. Principles for personal data processing, legal grounds for processing

16.2.1. Principles for personal data processing

16.2.1.1. Lawfulness, fairness and transparency principle

The Company ensures the implementation of the principle referred to in Article 5(1)(a) of the GDPR concerning the processing of data lawfully, fairly and in a transparent manner by ensuring the legal basis for the processing and the exercise of the rights of individuals including, in particular, informing individuals of the processing of their data as required by the GDPR. To this end, the Company, as part of its internal procedures, ensures the implementation of this principle.

16.2.1.2. Purpose limitation principle

The Company ensures that the principle of collecting data only for specific, explicit and legitimate purposes and not processing them further in a manner incompatible with those purposes, i.e. the principle referred to in Article 5(1)(b) of the GDPR, is implemented. To this end, the Company, as part of its internal procedures, ensures the implementation of this principle, in particular by providing adequate supervision in this regard, taking into account the roles and tasks of the Data Protection Officer.

16.2.1.3. Data minimisation principle

The Company ensures the implementation of the data minimisation principle referred to in Article 5(1)(c) of the GDPR by processing data that is adequate, relevant and limited to the purposes of the processing. To this end, the Company has internal processes in place to enforce this principle, including, in particular, ensuring that data minimisation requirements are taken into account in the development of new and modification of existing processes and systems as part of the identification of operational risks.

16.2.1.4. Accuracy principle

The Company ensures that the principle referred to in Article 5(1)(d) of the GDPR, according to which data should be correct and updated when necessary, is implemented. The Company will take all reasonable steps to ensure that personal data that is inaccurate in light of the purposes of its processing is promptly deleted or rectified. To this end, the Company ensures, as part of its internal procedures, the implementation of this principle, including, in particular, the management of the data used in the course of its business, which includes, for example, the management of data architecture and data quality, taking into account the periodic assessment of data quality, the cleaning of data, the identification of the causes of errors occurring in the data and the ongoing monitoring of data quality.

16.2.1.5. Storage limitation principle

The Company ensures the implementation of the principle referred to in Article 5(1)(e) of the GDPR, according to which data should be kept in a form which permits the identification of the data subject for no longer than is necessary for the purposes for which the data are processed. To this end, the Company, as part of its internal procedures, ensures the implementation of this principle and sees to it that the effectiveness and correctness of the controls in this regard take into account, in particular, the roles and tasks of the Data Protection Officer.

16.2.1.6. Integrity and confidentiality principle

The Company ensures data integrity and confidentiality as defined in Article 5(1)(f) of the GDPR by adequately ensuring the security of personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage by means of appropriate technical and organisational measures.

16.2.1.7. Accountability principle

The Company ensures the implementation of the principle of accountability referred to in Article 5(2) of the GDPR by putting in place appropriate procedures and policies to demonstrate compliance with the provisions of the GDPR, with particular reference to the participation of the Data Protection Officer in these efforts.

16.2.2. Our Assurances

For the effective implementation of the requirements of the GDPR, the Company provides:

a. technical measures and organisational solutions that are appropriate to the risks and categories of data to be protected;
b. training on the processing of personal data and methods of protecting it;
c. control and supervision of the processing of personal data;
d. monitoring of the protection measures taken.

16.2.3. Legal grounds for data processing

The Company processes personal data if at least one of the following conditions is met:

a. the data subject has consented to the processing of their personal data for one or more specified purposes;
b. the processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract;
c. the processing is necessary for the fulfilment of a legal obligation incumbent on the Company;
d. the processing is necessary to protect the vital interests of the data subject or of another natural person;
e. the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company;
f. the processing is necessary for the purposes of legitimate interests pursued by the Company or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

16.3. Data subject rights

The Company exercises the rights of data subjects, including:

a. the right to be informed (obligation to inform);
b. the right to access the data or to receive a copy of the data;
c. the right to rectification of data;
d. the right to erasure of data;
e. the right to restrict processing;
f. the right to data portability;
g. the right to object to processing.

16.4. Obligation to inform

In the event of the collection of personal data, as well as a change in the purposes of the processing of personal data in relation to the purpose for which the personal data were collected, the Company fulfills its obligation to provide information.

16.5. Data protection impact assessment

The Company assesses the effects of the planned processing operations on the protection of personal data where, according to the risk analysis, the risk of violation of the rights and freedoms of persons is high.

16.6. Security measures

The Company applies the security measures established through risk analyses and analyses of the adequacy of security measures and data protection impact assessments.

16.7. Reporting of violations

16.7.1. Data breach

A data breach at the Company is considered as an event occurring as part of operational risk, which is to be understood as the possibility of loss resulting from inadequate or unreliable internal procedures, people and systems or from external events.

16.7.2. Personal data breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, modification, unauthorised disclosure of or unauthorised access to personal data transmitted, stored or otherwise processed in the course of the Controller's business.

16.7.3. Personal data breach notification

A personal data breach that is notifiable:

a. to the supervisory authority – is considered to be a situation where the likelihood of a risk of violation of the rights or freedoms of individuals has been estimated by the Company to be higher than low;
b. to the data subject – is considered to be a situation in which the Company has assessed the risk of violation of the data subject's rights and freedoms to be high.

16.7.4. Situations identified as breach risk

In particular, the following situations may lead to a breach:

a. loss of personal data that prevents performance of the obligation;
b. breach of personal data integrity with a risk of incorrect performance of the obligation;
c. loss of confidentiality of personal data,

which may occur as a result of:

a. compromised or malfunctioning information system;
b. random/environmental incidents;
c. undesired (sabotage/disorganisation) actions of persons, including third parties (theft, destruction, preventing access, modification, disclosure of data);

d. human error, including as part of personnel misconduct in securing personal data.

16.7.5. Subject to the assessment of the risk of a breach

Subject to the assessment of the risk of a breach, a notifiable breach of personal data protection to the data subject may be, in particular: leakage (i.e. uncontrolled disclosure) of information from the database (a notifiable breach will not therefore be the leakage of a file containing only street names with numbers, only postal codes or city names), sending documents containing data constituting a legally protected secret by e-mail/traditional mail to an unauthorised person, interception and leakage of data/tools used for logging in and identifying individuals, loss/theft of documents containing individuals' data, breaking seals placed on containers used for archiving documents, generation and use of an erroneous database to send protected information to individuals, sending emails to uncovered recipients, information obtained by means of access to personal data by an unauthorised person.

16.7.6. Not notifiable personal data breach

A personal data breach not notifiable to the supervisory authority may be considered in particular: the leakage (i.e. uncontrolled disclosure) of information from a database that does not allow for the identification of a specific person, the loss of a data carrier with an encrypted file, where the key used to decrypt this data was not broken as a result of the breach.

16.7.7. Notification obligation

The notification obligation should be fulfilled without undue delay – if possible, no later than 72 hours after the breach is discovered. A breach is deemed to have been established when the Company, after promptly completing an investigation under its internal procedures, considers that the likelihood of a risk of violation of an individual's right and freedom has been assessed as higher than low. Whether notification has been made without undue delay shall be determined taking into account, in particular, the need to establish the causes and consequences of the breach and to minimise those consequences, the nature and gravity of the personal data breach, its consequences and adverse effects on the data subject. If the above time limit is not met, the notification must be accompanied by an explanation of the reason for the delay.

16.7.8. Risk assessment of a breach

Where a personal data breach would result in a high risk of harm to the rights or freedoms of individuals, the breach should be notified to data subjects without delay, and if such notification would require a disproportionate effort, a public notice of the breach should be issued.

16.7.9. Notifying an individual

Notification to the individual is not necessary if adequate protection measures have been implemented covering the personal data affected by the breach and measures have been taken to eliminate the likelihood of a high risk of violation of the rights or freedoms of data subjects.

16.7.10. Documentation

Documentation shall be drawn up of each personal data security breach, describing in particular:

a. circumstances of the breach, for example:
   - date and time the personal data breach was discovered;
   - description of the nature of the breach;
   - cause of the breach,

b. actual and likely consequences of the breach;

c. remedial measures taken.

16.8. Entrustment of processing - supplier agreements

16.8.1. Sufficient guarantees

The Company, when entrusting the processing of personal data, uses such suppliers that provide sufficient guarantees to implement appropriate technical and organisational measures so that the processing meets the requirements of the GDPR and protects the rights of the data subjects. Controllers, when selecting a data processor, pay attention to the security standards applied by the processor or set the standard they require (e.g. through audits or other forms of verification).

16.8.2. Legal basis

The entrustment of processing is carried out on the basis of an agreement or other legal instrument governed by European Union law or the law of a Member State, and the principles on the basis of which the entrustment is carried out satisfy the requirements of Article 28 of the GDPR.

16.9. Data export

The Company has a policy for verifying when cross-border processing occurs and a policy for determining the lead supervisory authority and the lead business unit within the meaning of the GDPR.

The level of protection of personal data outside the European Economic Area (EEA) may differ from that provided by European law. With this in mind, the Company only transfers personal data outside the EEA when necessary. In the event of such a transfer, the Company shall ensure an adequate level of protection of personal data primarily by:

a. the transfer of personal data to countries for which a European Commission decision recognising the country as providing an adequate level of protection for personal data has been issued;
b. the use of standard contractual clauses issued by the European Commission;
c. the use of other appropriate safeguards.

17. AI Policy

17.1. AI Integration in Trans.eu

Trans.eu embraces Artificial Intelligence (AI) as a strategic component in enhancing and developing its logistics platform. AI-powered tools are used to improve existing functionalities, develop new features, automate internal processes, and create tailored IT solutions that support business efficiency. These AI-driven innovations contribute to better decision-making, workflow automation, and customer experience enhancement.

17.2. Compliance and responsible AI use

Recognizing the potential and challenges associated with AI, Trans.eu ensures that all AI-based tools and systems, whether developed internally or sourced externally, comply with applicable legal regulations, including:

- The **AI Act** of the European Union, ensuring that AI applications align with transparency, accountability, and ethical guidelines - Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).
- The **General Data Protection Regulation (GDPR)**, ensuring that AI-driven data processing adheres to stringent privacy and security standards - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on

the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Every AI system deployed is assessed for compliance with these regulations, and internal audits are conducted to validate the security, fairness, and reliability of AI-driven processes.

17.3. Ethical AI and transparency

Trans.eu is committed to the responsible and ethical use of AI. The company upholds the following principles:

- **Transparency** – Customers and users are informed when interacting with AI-driven functionalities, ensuring clarity about AI's role in decision-making processes, if it plays such a role.
- **Accountability** – AI applications are monitored and evaluated to prevent bias, discrimination, and unintended consequences.
- **Data Integrity and Security** – AI models are designed to process data securely and with the highest confidentiality standards.
- **Human Oversight** – AI-driven decisions that may significantly impact users will be subject to human review to prevent errors and ensure fairness.

By integrating AI responsibly, Trans.eu aims to drive innovation while ensuring compliance, trust, and transparency for its users.

17.4. AI Risk assessment and mitigation

To ensure the safe and effective use of AI, Trans.eu applies a structured AI risk assessment framework that evaluates AI-powered tools and functionalities across multiple risk dimensions:

17.4.1. AI risk evaluation criteria

Each AI system is assessed based on:

- **Compliance Risk** – Ensuring adherence to the AI Act, GDPR, and other relevant legal frameworks.
- **Bias and Fairness Risk** – Evaluating models for potential biases that may lead to unfair or discriminatory outcomes.
- **Security Risk** – Assessing vulnerability to adversarial attacks, data leaks, and unauthorized access.
- **Data Privacy Risk** – Ensuring AI tools handle personal and business data in compliance with data protection regulations.
- **Operational Risk** – Assessing reliability, interpretability, and accuracy to minimize incorrect or misleading AI-generated outcomes.

17.4.2. Risk mitigation strategies

To address identified risks, Trans.eu employs the following **AI governance mechanisms**:

- **AI Model Testing & Validation** – All AI models undergo rigorous testing in controlled environments before deployment.
- **Bias Detection & Correction** – Regular audits are conducted to detect and mitigate biases within AI algorithms.
- **Explainability & Interpretability** – AI models used in decision-making provide clear justifications for their recommendations.
- **Incident Response & Monitoring** – AI-driven processes are continuously monitored to detect anomalies and ensure timely corrective action.
- **Ethical AI** – An internal team reviews high-risk AI applications to ensure compliance with ethical standards.

17.5. AI-powered customer-facing tools

Trans.eu integrates AI-driven features to enhance customer experience and operational efficiency. To improve customer support, Trans.eu deploys AI-driven chatbot that assist users with instant query resolution providing automated responses to common customer inquiries.

17.6. Continuous Improvement & Future AI Development

Trans.eu is committed to continuously improving its AI models by:

- Incorporating user feedback to refine AI recommendations.
- Regularly updating AI models to reflect changing logistics and regulatory landscapes.
- Collaborating with AI research institutions and industry experts to enhance AI adoption in logistics.

By maintaining an ethical, transparent, and compliance-driven approach to AI, Trans.eu ensures that artificial intelligence remains a tool for empowerment rather than risk.

18. Security measures for eCMR in the Trans.eu Platform

18.1. Characteristics of the eCMR solution

The eCMR module constitutes an integral part of the Trans.eu Platform, utilizing the shared infrastructure and security measures described in this document.

The purpose of the eCMR solution is to ensure a fully digital, secure, and legally compliant circulation of the electronic CMR consignment note.

The eCMR solution complies with the following legal acts:

- Additional Protocol to the CMR Convention,
- eIDAS Regulation with regard to the use of qualified electronic signatures,
- eFTI Regulation (European Freight Transport Information).

Trans.eu employs IBM Hyperledger Blockchain technology, which ensures a durable and immutable data register.

18.2. Authorization and access control model

The eCMR module utilizes the common user authorization process of the Trans.eu Platform, which includes, among others, two-factor authentication (2FA), a verification bank transfer of 1 PLN, and validation of company data (National Court Register – KRS, Tax Identification Number – NIP).

Within the eCMR solution, the following user roles are defined:

- Administrator,
- Manager,
- Employee,
- Payer (as defined in the eCMR Terms and Conditions).

The system supports the operation of multiple branches within a single organization, ensuring full data separation and controlled visibility of documents.

18.3. Document visibility and accessibility

Each eCMR document has a unique identifier and a complete record of all operations performed. The scope of document visibility among the parties involved in the transport process (consignor, carrier, consignee) depends on the stage of transport execution. Access to the document is automatically restricted after the transport is completed.

All user activities, including signatures, approvals, edits, PDF exports, and printouts, are recorded in the system logs as well as in the blockchain register.

18.4. Electronic signature and delivery confirmation

Signatures within the eCMR system can be executed only from authorized user accounts on the Trans.eu Platform.

For operations performed outside the system (for example, confirmation of goods release at the unloading point), a mechanism based on two unique authorization codes (SMS/e-mail) assigned to the consignor and the consignee is used. Only a person possessing the correct pair of codes can confirm the receipt of the goods.

To enable participation of entities not registered on the Trans.eu Platform, the eCMR module employs a secure authorization mechanism using SMS or e-mail codes. This allows external partners to confirm loading or unloading activities without the need for an account, while ensuring full traceability of actions.

The process involves sending unique codes assigned to a specific eCMR document to the contact persons designated for each partner. Once the carrier enters the correct codes, the signature is automatically recorded in the appropriate section of the document.

An extension of this functionality is planned to enable full user identification within the document fields and the operation history.

18.5. Technical security and compliance

The eCMR solution operates within the infrastructure of the Trans.eu Platform, hosted in data centers managed by Talex (Poland) and AWS (Luxembourg). User data is processed within the territory of the European Union.

All data is encrypted both during transmission (using the TLS protocol) and at rest (using the AES standard), in accordance with the principles described in Section 8. Data Encryption.

The eCMR module is subject to regular security assessments and penetration tests, as outlined in Section 2.3. Audit Scope.

Each eCMR document in PDF format is assigned a unique identifier that enables unambiguous verification of its origin.

18.6. Interfaces and integrations

The eCMR module provides an API interface that enables integration with external systems such as WMS or TMS.

Additionally, the “Smart Importer” functionality is available, allowing data import from files in CSV or XLS formats.

In exceptional cases, it is also possible to obtain a paper version of the document, in accordance with Article 4 of the Additional Protocol to the CMR Convention.

18.7. Security incident management

Incidents related to the eCMR module are handled in accordance with the procedures described in Section 12. Incident Management.

All reports are analyzed by the Trans.eu Security Team, and in cases requiring legal intervention, also by the Legal Department and the Data Protection Officer (DPO).