

Privacy Policy

for the National Integrated Travel Ticket (NICT) services / CYRIL application

Item	Value
Controller	Ministry of Transport of the Slovak Republic, National Transport Authority
Service	NICL / CYRIL
Version	1.0 first publication
Date of last update	25.06.2026
Language version	English

Contents

1. Purpose and scope of the policy	4
2. Controller and contact details	4
3. NICL / CYRIL services and data subjects	4
4. Categories of personal data and purposes of processing	5
4.1 Registration and management of the user account	5
4.2 Purchase of travel documents and purchase history	5
4.3 Payments	6
4.4 Discounts and tariff categories	6
4.5 PAYGO and technical Bluetooth data	6
4.6 Inspection of the passenger	7
4.7 Complaints, grievances, suggestions and customer support	7
4.8 Technical logs, security and system operation	7
4.9 Notifications, communication and marketing	8
5. Legal bases for processing	8
6. Recipients, processors and partners	9
7. Transfers of personal data outside the EU/EEA	10
8. Personal data retention periods	10
9. Technical and organisational security measures	11
10. Automated processing and profiling	11
11. Rights of data subjects	12
12. Cookies, analytics and mobile permissions	12
13. Children, minor users and discounted fares	13
14. Updating of the policy and availability of the document	13
Annex No. 1 - Summary table of personal data processing	13

1. Purpose and scope of the policy

This privacy policy (hereinafter the „policy“) informs data subjects about how the Ministry of Transport of the Slovak Republic, National Transport Authority Department, processes personal data in the provision of the NICL / CYRIL services, which are part of the single travel ticket solution in the territory of the Slovak Republic.

The purpose of the policy is to fulfil the controller's information obligation under Articles 13 and 14 of Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter the „GDPR“) and under Act No. 18/2018 Coll. on the protection of personal data.

The policy applies in particular to the use of the CYRIL mobile application for the Android and iOS operating systems, the web portal, the e-shop, the user account, the complaint form, customer support, the contact form, the control interfaces for carriers and inspectors, and the internal interfaces used for system administration, the handling of complaints, user support, reporting and the operational management of the services.

2. Controller and contact details

The controller of the NICL information system and the processor of personal data is the Ministry of Transport of the Slovak Republic, National Transport Authority Department, which determines the purposes and means of processing personal data within the NADA / NICL / CYRIL services.

Data	Value
Controller	Ministry of Transport of the Slovak Republic, National Transport Authority Department
Registered office	Námetie slobody 2902/6, 810 05 Bratislava, Slovak Republic
Company ID (IČO)	30416094
E-mail of the data protection officer	dpo@mindop.sk
Electronic mailbox	via the Central Public Administration Portal slovensko.sk
Complaints and suggestions regarding the service	a separate complaint or contact form available in the NICL / CYRIL services

The National Transport Authority (hereinafter „NADA“) is an organisational unit of the Ministry of Transport of the Slovak Republic without separate legal personality. NADA ensures the substantive, methodological and coordination activities related to the single travel ticket services and the related NICL / CYRIL systems. The controller of personal data remains the Ministry of Transport of the Slovak Republic.

3. NICL / CYRIL services and data subjects

The IS NICL application platform is available in the public distribution channels Google Play and Apple App Store under the user name „CYRIL“. In this policy, the designation „NICL / CYRIL“ is used for the system, application and user interface through which a passenger uses the single travel ticket services, the user account, the purchase of travel documents and related services.

The NICL / CYRIL services are intended for the provision of single travel ticket services in the territory of the Slovak Republic. They apply to public passenger transport involved in the single

travel ticket system, in particular rail transport, suburban bus transport, urban public transport and integrated transport systems. The services do not apply to cross-border or international journeys, unless expressly stated otherwise in a specific service or in the terms and conditions.

The NICL / CYRIL services enable in particular the registration and management of a user account, the purchase of single and time-based travel documents, the use of discounted fares, the purchase of a travel document for another person or fellow passenger, the use of the PAYG mode, the payment of fares by available payment methods, the issuance of a tax document or proof of purchase, the management of journey and purchase history, the receipt of notifications, and the lodging of complaints, cancellation requests or refund requests.

Categories of data subjects

- registered users of the application or web portal;
- unregistered users, if they use the service without registration;
- passengers for whom a travel document was purchased by another person;
- fellow passengers within a single purchase or journey;
- children, minor users and their legal representatives;
- persons claiming an entitlement to a discount;
- persons lodging a complaint, grievance or suggestion;
- persons communicating with customer support;
- persons inspected by an inspector or carrier;
- employees of carriers or integrated transport systems using the control, operational or reporting interface.

4. Categories of personal data and purposes of processing

The scope of the personal data processed depends on the specific service that the user uses and on their role within the NICL / CYRIL services.

4.1 Registration and management of the user account

For the purposes of registration, creation, verification and management of the user account, the following are processed in particular: first name, surname, date of birth, e-mail address, telephone number, login name or user ID, technical account identifier, authentication data, preferred language, history of consents granted or withdrawn, account status, device identifier and IP address.

If a password is used to log in, the password is not processed in a readable form. It is stored in a technically secured manner, in particular in the form of a cryptographic hash or another appropriate security mechanism. If a one-time verification code sent by e-mail is used, the system processes the data necessary for its delivery, verification and the recording of the success or failure of the authentication.

4.2 Purchase of travel documents and purchase history

For the purposes of the purchase, issuance, recording, management, inspection and use of travel documents, the following are processed in particular: data on the type of travel document, the number or other identifier of the travel document, the date and time of purchase, the date and time of validity, the boarding and destination stop or zone, the route or tariff combination, the carrier or the integrated transport system involved, the fare, the discount or tariff category, the tax document or invoicing data, purchase history, data on the fellow passenger or the person for

whom the travel document was purchased, the status of the travel document, and the link to the payment or the payment transaction identifier.

4.3 Payments

For the purposes of paying the fare, processing payments, recording payment transactions, issuing proof of payment, and handling a complaint, cancellation or refund, the following are processed in particular: data on the payment method, the payment transaction identifier, the payment token, the payment status, the date and time of the payment, the amount paid, the currency, the link of the payment to a travel document or user account, and information about an unsuccessful, rejected or cancelled payment.

Payment data is processed via an external payment gateway or payment service providers. The NICL / CYRIL services do not store the full payment card number or the card security code. Only the data necessary to identify and manage the payment method may be stored in the system, for example the payment token, the transaction identifier, the last four digits of the payment card, the type of payment method and the payment status.

The user may use payment by payment card, Apple Pay or Google Pay. If the user saves a payment method for repeated purchases or for the use of the PAYG mode, the system processes the technical data necessary for the repeated or subsequent settlement of the payment. When using the PAYG mode, the fare may be charged automatically after the use of the service has ended or after the price has been determined according to the rules of the service.

4.4 Discounts and tariff categories

For the purposes of claiming a discounted fare, the data necessary to assign and apply the relevant tariff or discount category are processed. This may include in particular: the date of birth, the status of a pupil, student, senior, pensioner, person with a severe disability or another person entitled to a discount under the relevant legal regulations or tariff rules, the type of discount or the tariff category, and the date of validity of the discount entitlement, if it is necessary for the issuance or use of the travel document.

For persons with a severe disability or with a severe disability with an escort, the diagnosis, medical documentation, photograph, scan of the document, image of the card or the number of the ŤZP / ŤZP-S card is not processed. The system processes only the information on the relevant tariff or discount category, if it is necessary for the issuance or use of a discounted travel document.

The entitlement to a discount is not verified in the NICL / CYRIL services against an external register or through the storage of the user's documents. The eligibility for the use of the discount may be checked only during a transport inspection by an inspector or an authorised person of the carrier, according to the rules of the relevant carrier and the tariff conditions.

4.5 PAYGO and technical Bluetooth data

When using the PAYGO mode / automatic recording of the use of the service, the start and end of the use of the service is not activated manually by the user via the check-in / check-out function. The start of the use of the service is recorded automatically on the basis of a technical connection or the recognition of the relevant Bluetooth element. The use of the service ends automatically upon the loss of the relevant Bluetooth connection.

For this purpose, the NICL / CYRIL services do not use the GPS location of the user's mobile device, do not collect location data before the journey, during the journey or after its end, and do not use data from the mobile device's motion sensors. The system does not process data on the user's

precise geographical location, nor does it calculate the route travelled, the stops, zones or carrier on the basis of GPS or motion data.

The system processes technical data related to the Bluetooth connection or the recognition of a Bluetooth element, in particular: the identifier of the Bluetooth element or beacon, the time of connection to or recognition of the Bluetooth element, the time of disconnection or loss of the Bluetooth connection, the carrier data derived from the relevant Bluetooth element, the technical identifier of the user's mobile device, and the user account identifier.

In this mode, the vehicle ID, the line, the specific service, the route travelled, the stops, the zones, the resulting fare or a record of the successful charging of the journey are not processed as part of the Bluetooth record. Bluetooth data is not used to track the user's movement, to profile their location, or to calculate a route based on geographical location.

4.6 Inspection of the passenger

During the inspection of the validity of a travel document via the control interface or the control application, only the data necessary to verify the validity of the travel document are processed. This includes in particular: the QR code or another control identifier of the travel document, the ID of the travel document, the status of the travel document, the type of discount or the tariff category, the validity time of the travel document, the carrier or integrated transport system, and the zone, relation or other territorial validity of the travel document.

During a standard inspection of a passenger, the control interface does not make available the passenger's first name and surname, the passenger's date of birth, the history of previous journeys or purchases, the reason for the invalidity of the travel document, the identifier of the inspector or control device, or the result of the inspection. The control interface serves exclusively to verify whether the travel document is valid for the specific transport, discount, time period, zone, relation or carrier.

4.7 Complaints, grievances, suggestions and customer support

For the purposes of receiving, recording, assessing and handling complaints, grievances, suggestions, cancellation requests, refund requests and user requirements, the following are processed in particular: the first name and surname of the person lodging the complaint or suggestion, the e-mail address, the telephone number, the user account identifier, the travel document identifier, the payment transaction identifier, the description of the complaint, grievance or suggestion, attachments submitted by the user, the content of communication with customer support, the status of the handling of the complaint, the result of the handling of the complaint, the data necessary for the refund, the internal notes of the support employee, and the user's complaint history.

4.8 Technical logs, security and system operation

For the purposes of ensuring the operation, availability, integrity, security and auditability of the NICTL / CYRIL services, technical and operational data are processed to the necessary extent. This includes in particular: the user's IP address, the date and time of the user's login and logout, records of unsuccessful login attempts, the version of the CYRIL application, the technical device identifier, application logs, system logs, security logs, administrator logs, records of account or user setting changes, records of application errors and crashes, and the data necessary to resolve security incidents.

For this purpose, the NICL / CYRIL services do not process the type of device or the operating system of the device, unless this data is necessary and technically processed in a specific operational, security or diagnostic component of the system.

4.9 Notifications, communication and marketing

For the purposes of informing users about the NICL / CYRIL services, the status of the user account, travel documents, payments, complaints and security events, the following are processed in particular: the e-mail address, the data necessary to deliver a push notification in the mobile application, the user account identifier, the travel document identifier, the payment identifier, the status of the complaint, and other data necessary to deliver the relevant service or security message.

The NICL / CYRIL services may send the user service e-mail notifications, confirmations of the purchase of a travel document, confirmations of payment, notifications on the status of a complaint, alerts about the approaching end of the validity of a travel document or subscription, security alerts concerning the account, and push notifications in the mobile application. SMS service notifications are not used.

Marketing or information campaigns, the newsletter, marketing profiling and user satisfaction surveys are carried out only on the basis of the relevant legal basis, in particular the user's consent. The user may withdraw their consent to marketing communication or to the subscription of the newsletter at any time, or unsubscribe from such communication.

5. Legal bases for processing

Purpose	Legal basis
Registration and management of the user account	performance of a contract or pre-contractual measures – Art. 6(1)(b) GDPR
Purchase, issuance and recording of a travel document	performance of a contract – Art. 6(1)(b) GDPR
Tax and accounting documents	compliance with a legal obligation – Art. 6(1)(c) GDPR
Payments	performance of a contract and, for accounting obligations, compliance with a legal obligation – Art. 6(1)(b) and (c) GDPR
PAYG and technical Bluetooth records	performance of a contract – Art. 6(1)(b) GDPR
Discount or tariff category	performance of a contract, compliance with a legal obligation or performance of a task carried out in the public interest, depending on the type of discount – Art. 6(1)(b), (c) or (e) GDPR
Inspection of the passenger and verification of the validity of the travel document	performance of a contract and legitimate interest in checking the authorised use of the transport service – Art. 6(1)(b) and (f) GDPR
Complaints, grievances, suggestions, cancellation and refund	performance of a contract, compliance with a legal obligation and legitimate interest in the proper handling of the request and the protection of legal claims – Art. 6(1)(b), (c) and (f) GDPR

Technical, operational, security and administrator logs	legitimate interest in the secure, reliable and auditable operation of the services; for legal obligations also Art. 6(1)(c) GDPR
Service notifications	performance of a contract or legitimate interest – Art. 6(1)(b) or (f) GDPR
Marketing communication, newsletter, marketing profiling, analytical and marketing cookies	consent of the user – Art. 6(1)(a) GDPR
Necessary technical cookies	necessity of providing the service or legitimate interest in a functional and secure web interface – Art. 6(1)(f) GDPR
Profiling of travel behaviour for statistical, analytical, operational and development purposes	legitimate interest – Art. 6(1)(f) GDPR; for marketing use, the consent of the user

6. Recipients, processors and partners

Personal data may, to the necessary extent, be made available or provided to recipients, separate controllers or processors, where this is necessary to provide the services, ensure transport, verify the validity of travel documents, settle revenues, process payments, handle complaints, for technical operation, system security, compliance with legal obligations or the protection of legal claims.

Carriers, organisers of integrated transport systems and other partners involved act as separate controllers of personal data in the provision of transport services, the inspection of passengers, the handling of complaints, the settlement of revenues, statistics, reporting and the fulfilment of their legal or contractual obligations. A specific list of carriers is not provided in this policy.

Through the NICL / CYRIL services, the Ministry of Transport of the SR makes available to them only personal data to the necessary extent, in particular for the purposes of verifying the validity of the travel document, identifying eligibility for travel during an inspection, resolving complaints, settling revenues, statistics and reporting.

Contractual processors and technical suppliers may participate in the processing of personal data, in particular providers of cloud services, the government cloud, technical operation, support, e-mail and notification services, analytical tools, marketing tools, crash reporting and security services. These processors process personal data exclusively on the instructions of the Ministry of Transport of the SR and under the conditions set out in Art. 28 GDPR.

The technical supplier of the system does not have access to the production personal data of users. Development, testing and service activities are carried out without the use of real production personal data. The production environment is separated from the testing and development environment.

Payments may be processed via a payment gateway provider or payment service providers. When using Apple Pay or Google Pay, the relevant providers of these services may also participate in the processing of data according to their own privacy rules. In the distribution of the mobile application, the provision of platform services, push notifications and certain technical functions, the companies Apple and Google may also be involved as operators of mobile platforms or providers of related technical services.

Personal data may be provided to public authorities, courts, law enforcement authorities, supervisory authorities or other authorised entities, if such an obligation is established by a legal regulation or if it is necessary to protect legal claims. To a reasonable extent, the data may also be

made available to legal, audit, accounting or professional advisors bound by a duty of confidentiality.

7. Transfers of personal data outside the EU/EEA

Personal data processed within the NICL / CYRIL services is processed primarily within the European Union or the European Economic Area.

The technical operation of the services is ensured through cloud services operated within the EU, including Microsoft Azure services in data centres in the EU and the government cloud operated in the Slovak Republic or within the EU.

The Ministry of Transport of the SR does not anticipate the transfer of personal data processed within the NICL / CYRIL services to third countries outside the European Union or the European Economic Area, nor to international organisations. The technical, analytical, marketing, notification and platform services used are set up so that the processing of personal data takes place within the EU/EEA.

8. Personal data retention periods

Personal data is retained only for the period necessary to achieve the purpose for which it was obtained, or for the period required by the relevant legal regulations.

Category of data	Retention period
User account	for the duration of the user account
Data after account cancellation	erasure or anonymisation without undue delay, except for legal exceptions, complaints, disputes, security incidents or accounting and tax obligations
Travel documents	at most 12 months from the end of the validity of the travel document, unless a special legal regulation or a legitimate purpose requires longer retention
Purchase history	for the duration of the account, but at most according to the retention period of the relevant travel document, unless it is an accounting or tax document
PAYG / Bluetooth records	at most 12 months from the use of the service or the end of the validity of the travel document
Accounting and tax documents	for the period required by accounting and tax regulations, generally 10 years
Payment transactions linked to an accounting document	generally 10 years or according to accounting and tax obligations
Complaints, grievances, suggestions	for the period necessary to handle the request and subsequently according to the records management plan or for the period necessary to protect legal claims
Technical logs	a reasonable operational period according to the internal settings of the system

Security logs	according to security and audit rules; in the event of a security incident, longer, if necessary
Administrator logs	according to audit and security rules
Crash logs	for the period necessary to diagnose and rectify the error
Marketing consents	until the consent is withdrawn
History of consents	for the period necessary to demonstrate compliance with the obligations under the GDPR

Data under § 6(g) and (h) of Act No. 332/2023 Coll. is retained for at most 12 months from the end of the validity of the national integrated travel ticket, unless a special legal regulation or a legitimate purpose of processing requires a longer retention period.

9. Technical and organisational security measures

The Ministry of Transport of the SR adopts appropriate technical and organisational measures to protect the personal data processed within the NICL / CYRIL services. The aim of these measures is to ensure the confidentiality, integrity, availability and resilience of the systems and services, as well as the protection of personal data against unauthorised access, loss, misuse, alteration or unauthorised disclosure.

- encrypted communication between the mobile application, the web interface and the server part of the system,
- separation of the production, testing and development environments,
- non-use of production personal data for development and testing,
- management of access permissions and multi-factor authentication for administrators,
- logging of administrator and security-relevant activities,
- backup of the system and data and appropriate protection or encryption of backups,
- monitoring of security events, regular updates and security patches,
- security testing including penetration testing,
- incident management procedures and rules for resolving security incidents,
- minimisation of the data processed and the use of anonymisation or pseudonymisation where possible and appropriate.

Access to production systems and personal data is limited to authorised persons according to their work or contractual role and the need for access. Administrator and security-relevant activities are logged and may be subject to inspection, audit or security evaluation.

10. Automated processing and profiling

The NICL / CYRIL services may use automated data processing in ensuring selected functions of the system, in particular in the automatic assignment of a carrier according to a recognised Bluetooth element, the automatic settlement of payment in the PAYG mode and the protection of the system against misuse.

In the event of the identification of a suspicion of misuse of the service, automated blocking of the user account or a restriction of certain functions of the service may occur. In such a case, the user has the option of lodging a complaint, suggestion or request for a review of the blocking via the complaint or contact form, or in another manner set out in this policy. The blocking of the account

may subsequently be manually reviewed by an authorised support employee or the administrator of the service.

Marketing profiling of the user is carried out only on the basis of their consent. The user may withdraw their consent to marketing profiling at any time in the user account, in the settings of the service, via the relevant link in the marketing communication, or in another available manner set out in the service.

Profiling of users' travel behaviour may be carried out for analytical, statistical, operational and development purposes, in particular for evaluating the use of the services, planning the development of the single travel ticket, improving the user experience and optimising the services. For these purposes, anonymised or pseudonymised data is used whenever this is possible and appropriate in view of the purpose of the processing.

11. Rights of data subjects

In connection with the processing of personal data, the data subject has rights under the GDPR, in particular the right of access to personal data, the right to rectification of incorrect or incomplete personal data, the right to erasure of personal data, the right to restriction of processing, the right to data portability, the right to object to processing, the right to withdraw consent to the processing of personal data if the processing is based on consent, and the right to lodge a complaint with a supervisory authority.

The data subject may exercise their rights with the Ministry of Transport of the SR by e-mail at dpo@mindop.sk, via the electronic mailbox of the Ministry of Transport of the SR at slovensko.sk, in writing at the address Ministry of Transport of the Slovak Republic, Námetie slobody 2902/6, 810 05 Bratislava, or via the complaint or contact form available in the NICL / CYRIL services, if such a form is designated for the given type of request.

The Ministry of Transport of the SR will handle the data subject's request without undue delay, at the latest within one month of its receipt. In justified cases, in particular in view of the complexity or number of requests, this period may be extended in accordance with the GDPR. The data subject will be informed of the extension of the period and the reasons for the extension.

If the Ministry of Transport of the SR has reasonable doubts about the identity of the person exercising the rights of the data subject, it may request the provision of additional information necessary to confirm the identity of the applicant. The purpose of verifying identity is to protect personal data against unauthorised disclosure or unauthorised interference.

If personal data is processed on the basis of consent, the data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of the processing carried out before its withdrawal.

The data subject also has the right to contact the Office for Personal Data Protection of the Slovak Republic if they believe that the processing of their personal data has infringed the legal regulations in the area of personal data protection.

12. Cookies, analytics and mobile permissions

When using the web portal or e-shop of the NICL / CYRIL services, cookies and similar technologies may be used. Necessary technical cookies are used to ensure the basic functionality of the web interface, user login, security, session retention and the proper functioning of the services provided. These cookies are necessary to provide the service and do not require the user's consent.

Analytical cookies and marketing cookies are used only on the basis of the user's consent, if such consent is granted via a cookie bar or another consent management tool. The user may change or withdraw their consent at any time.

In the CYRIL mobile application, tools for application usage analytics, crash reporting and the delivery of push notifications via services provided by the operators of the mobile platforms Apple and Google may be used. These tools are used in particular to improve the stability and functionality of the application, to detect and rectify technical errors, to evaluate the use of individual functions and to deliver service or security alerts to the user.

The CYRIL mobile application uses the Bluetooth permission, which is necessary for the recognition of or connection to the relevant Bluetooth element when using selected services, in particular the PAYG mode. The application does not use the permission for GPS or the determination of the user's geographical location, the permission for the camera, the permission for contacts, or biometric verification via Face ID, Touch ID or similar technology of the device. If the operating system of the mobile device technically requires the granting of a permission related to Bluetooth or nearby devices, this permission is used exclusively for the purposes of the technical recognition of a Bluetooth element and not for the determination of the GPS location or the tracking of the user's movement.

13. Children, minor users and discounted fares

A user account of a child or minor may be created by a legal representative. A minor user may use their own account independently from the age of 15, if the conditions of the service and the relevant legal regulations allow it. For users younger than 15, the involvement of a legal representative is required.

When claiming a discounted fare, only the data necessary to assign and apply the relevant tariff or discount category are processed. If the discount category is associated with a special status of the passenger, the system processes only the information on the relevant category to the necessary extent, not the underlying documents or specific details about the health, social or other personal status of the passenger.

14. Updating of the policy and availability of the document

This policy may be updated, in particular upon a change in the scope of the NICL / CYRIL services, a change in the categories of personal data processed, a change in the legal bases for processing, the involvement of significant new recipients or processors, a change in retention periods, a change in technologies or upon a change in legal regulations.

The current version of the policy is available on the website of the service and in the CYRIL mobile application. The document is also available in a form suitable for download. The user may be informed of significant changes to the policy via the application, e-mail communication, the web portal or in another appropriate manner.

The controller keeps an internal record of changes to this document. Before publication and upon significant changes to the services, an appropriate data protection impact assessment is carried out, including a DPIA screening or an impact assessment, if this is necessary under the GDPR.

Annex No. 1 - Summary table of personal data processing

Area	Categories of data	Purpose	Legal basis	Period
------	--------------------	---------	-------------	--------

User account	first name, surname, date of birth, e-mail, telephone, account ID, authentication data, language, consents, account status, device ID, IP address	creation and management of the account, authentication, account security	Art. 6(1)(b), (f) GDPR	for the duration of the account
Travel documents	type and ID of the ticket, time of purchase and validity, zones, relation, tariff combination, carrier/IDS, price, tariff category, ticket status	purchase, issuance, recording, inspection, purchase history	Art. 6(1)(b), (c), (f) GDPR	at most 12 months from the end of validity, unless a legal exception applies
Payments	payment method, token, transaction ID, payment status, amount, last 4 digits of the card	payment of the fare, proof of payment, complaints, cancellation	Art. 6(1)(b), (c), (f) GDPR	generally 10 years for accounting documents
PAYG / Bluetooth	Bluetooth element ID, connection and disconnection times, carrier, device ID, account ID	recording the use of the service and assignment to the account/carrier	Art. 6(1)(b) GDPR	at most 12 months from the use of the service
Discounts	tariff or discount category, date of birth, relevant status, validity of the entitlement	claiming a discounted fare and checking eligibility	Art. 6(1)(b), (c) or (e) GDPR	according to the validity of the entitlement and the retention period of the ticket
Inspection of the passenger	QR/control identifier, ticket ID, ticket status, tariff category, validity time, carrier/IDS, zone/relation	verification of the validity of the travel document	Art. 6(1)(b), (f) GDPR	only to the extent necessary for the inspection; without creating a record of the inspection in standard mode
Complaints and support	first name, surname, e-mail, telephone, account ID, ticket ID, payment ID, description, attachments, communication, status, result, notes, complaint history	receipt, assessment and handling of a complaint, suggestion, cancellation or refund	Art. 6(1)(b), (c), (f) GDPR	according to the handling of the request, the records management plan and the protection of legal claims

Technical and security logs	IP address, login/logout times, unsuccessful attempts, application version, device ID, application, system, security and administrator logs, crash logs	security, availability, auditability, resolution of errors and incidents	Art. 6(1)(c), (f) GDPR	according to internal security and operational rules
Marketing and analytics	e-mail, consents, service usage data, analytical and marketing identifiers according to the consent settings	newsletter, campaigns, surveys, marketing profiling, analytics	Art. 6(1)(a) GDPR; for necessary cookies Art. 6(1) (f) GDPR	until the consent is withdrawn or according to the rules on cookies and the recording of consents