

PRIVACY POLICY

Last Updated: June 26, 2026

INTRODUCTION

This Privacy Policy (“**Policy**”) explains how ProdigyChain, j.s.a., a simple joint-stock company duly organized and existing under the laws of the Slovak Republic, with its registered office at Karpatská 7, 911 01 Trenčín, Slovak Republic, BIN: 56 782 888, registered with the Commercial Register maintained by the District Court Trenčín, Section: Sja, Insertion no.: 23/R (“**ProdigyChain**”, “**we**”, “**our**”, “**us**”), collects, processes, stores and discloses your Personal Data in connection with the use of the ProdigyChain Platform (“**Platform**”).

ProdigyChain is the developer and operator of the Platform. This Policy is provided in accordance with Articles 13 and 14 of the GDPR and is intended to fulfil our obligations to inform data subjects about the processing of their Personal Data.

By creating an account, accessing, or otherwise using the Platform, you (“**User**”, “**you**”, “**your**”) acknowledge and agree that your personal data may be collected, processed, stored, and disclosed in accordance with this Policy. If you do not agree with this Policy, you must refrain from accessing or using the Platform.

1 DEFINITIONS

For purposes of this Policy, capitalized terms shall have the same meaning as defined in the Terms, supplemented by additional definitions required for data protection compliance. The following definitions apply, presented in alphabetical order:

“**Account**” shall mean a unique account created for You to access our Platform or parts of our Platform.

“**Cookies**” shall mean small files that are placed on Your computer, mobile device, or any other device by a website, containing browsing details and preferences.

“**General Data Protection Regulation**” or “**GDPR**” shall mean 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).

“**Personal Data**” shall mean any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“**Service Providers**” means third-party companies or individuals engaged to provide services on our behalf, including payment processing, identity verification, hosting, analytics, and compliance services.

“**Usage Data**” shall mean data collected automatically when using the Platform, including log files, IP address, device information, browser type, and activity metrics.

2 COLLECTING AND USING PERSONAL DATA

2.1 Categories of Personal Data Collected

We may collect and process the following categories of Personal Data:

- 2.1.1 Identification Data: including your name, date of birth, nationality, and government-issued identification documents;
- 2.1.2 Contact Data: including your email address, telephone number, and postal address;
- 2.1.3 Financial Data: including your bank account details, payment card information, payout details, and any related billing information;
- 2.1.4 NIL and ProdigyCard Data: including information concerning your participation in Name, Image and Likeness (NIL) activities, ProdigyCards, Donations, and any transactions or engagements on the Platform;
- 2.1.5 Guardian Data: in the case of Minors, identity and contact details of Guardians, along with consent records and verification documentation;
- 2.1.6 Verification Data: including documents and information required for KYC/AML checks;
- 2.1.7 Usage Data: information automatically collected when using the Platform, such as IP address, device type, operating system, browser type and version, geolocation data, referring websites, time and date of access, pages visited, and log files;
- 2.1.8 Communications Data: records of communications between you and us, including customer support inquiries, Guardian notifications, and other correspondence.

2.2 Sources of Personal Data

Personal Data may be obtained directly from you, generated automatically through your interactions with the Platform, or received from third parties, including but not limited to Service Providers (e.g., Payment Processors, hosting providers, identity verification services) and social media platforms if you choose to link your accounts.

2.3 Purposes of Processing Personal Data

We process Personal Data for the following purposes:

- 2.3.1 Provision of Services: to register and maintain your Account, enable the creation, acquisition, and trading of ProdigyCards, facilitate Donations, and deliver associated services on the Platform;

- 2.3.2 Compliance: to comply with applicable legal and regulatory obligations, including AML, KYC, tax, accounting, and reporting obligations;
- 2.3.3 Guardian Oversight: to verify and record Guardian consent and enable oversight of Minors' activities on the Platform;
- 2.3.4 Security and Integrity: to detect, prevent, and address fraud, abuse, technical issues, or unauthorized access;
- 2.3.5 Communications: to contact you regarding Platform use, updates to the Terms or this Policy, or information concerning our services;
- 2.3.6 Analytics and Improvements: to monitor and analyze usage trends, evaluate and improve the Platform, and develop new features;
- 2.3.7 Marketing: where you have provided explicit consent, to send promotional materials, newsletters, or offers tailored to your interests.

2.4 Protection of Minors

We apply enhanced safeguards when processing Personal Data of Minors. For additional safeguards applying specifically to Minors, see Article 12 (*Children's Privacy Enhanced Protections*).

- 2.4.1 Guardian consent must be verified before any account is activated for a Minor;
- 2.4.2 all financial transactions initiated by a Minor require Guardian approval, and any payouts are directed only to Guardian-verified accounts;
- 2.4.3 Personal Data of Minors is collected and retained on a strict "data minimization" basis and is never publicly disclosed;
- 2.4.4 Guardians are provided with oversight tools, including account monitoring, activity logs, and notifications;
- 2.4.5 all processing of Minors' Personal Data is conducted in accordance with Article 8 of GDPR, and any other applicable local legislation.

2.5 Sharing and Disclosure of Personal Data

In general, Personal Data may be shared with third parties in accordance with this Policy. For details regarding the categories of recipients and the circumstances under which Personal Data may be shared, please refer to Article 6 (*Sharing of Personal Data*) and Article 9 (*Disclosure of Personal Data*).

2.6 Retention of Personal Data

Personal Data will be retained only for as long as necessary to fulfil the purposes described in this Policy or as required by law. Specific retention periods and criteria are described in Article 7 (*Retention of Personal Data*) and in Appendix 1 (*Data Retention Schedule*).

2.7 Legal Bases for Processing Personal Data

The processing of Personal Data by us is based on lawful grounds under Article 6 of the GDPR, including contract performance, compliance with legal obligations, legitimate interests, and consent where applicable. A detailed explanation of these legal bases and how they apply is set out in Article 15 (*Legal Bases for Processing (GDPR)*)

3 PERSONAL DATA COLLECTION AND PROCESSING FOR SPECIFIC USER TYPES

This Section sets out the specific data collection and processing practices applicable to different categories of Users on the Platform, in addition to the general practices described in Article 2.

3.1 Student Athlete

3.1.1 Personal Data Collected:

- (i) Registration Data: email address, chosen sport or artistic activity, and, where provided, linked social media accounts (e.g., Instagram, Facebook);
- (ii) Profile Information: first name, last name, date of birth, nationality, player position (if applicable), current team, link to statistics page, short biography or list of achievements, academic information including school name and uploaded transcripts;
- (iii) Subscription Data: details relating to subscription status, payment history for premium templates and services;
- (iv) ProdigyCard Data: details relating to the creation and minting of ProdigyCards, including all associated NIL data;
- (v) Donation Preferences: information concerning designated sport organizations and charities selected for Donation sharing;
- (vi) Communication Data: records of interactions with the ProdigyChain community, including messages, posts, and other engagement data; and
- (vii) Guardian Information (for Minors): Guardian's contact details, consent records, and verification documents.

3.1.2 Purpose of Collection:

- (i) to create and manage the User's profile and Account;
- (ii) to facilitate the creation, minting, and management of ProdigyCards;
- (iii) to enable NIL monetization and charitable fundraising;
- (iv) to provide educational resources and networking opportunities;

- (v) to personalize the User's experience, including display of statistics and achievements;
- (vi) to process subscription fees and manage access to the ProdigyVault;
- (vii) to comply with financial, AML, and tax obligations;
- (viii) to enable communication and interaction within the ProdigyChain community; and
- (ix) to ensure proper Guardian oversight and compliance for Minors.

3.1.3 Personal Data Sharing:

- (i) certain profile elements (e.g., name, sport, achievements) may be publicly visible on User profiles to facilitate connections with donors, sponsors, and brands;
- (ii) for Minors, contact details are never made publicly available;
- (iii) Donation preferences are used exclusively for distribution of funds to designated beneficiaries;
- (iv) academic information may be used internally for "ProdigyPoints" calculations and may be shared with scholarship providers or educational institutions with explicit consent (and Guardian consent in the case of Minors);
- (v) with Service Providers (e.g., Stripe) and affiliates; and
- (vi) Guardian information is shared only for verification and compliance purposes.

3.2 Organizations (Combined User Category)

This category includes sport teams and clubs, schools and educational institutions, federations and governing bodies, sport events and competitions, spring or split season teams and similar types of organizations.

3.2.1 Personal Data Collected:

- (i) Organizational Information: full legal name, registration number, organizational type, and sport/activity affiliation;
- (ii) Contact Data: primary contact person's name, title or profession, verified email address, verified phone number, and registered address;
- (iii) Digital Presence: official website and optional social media links;
- (iv) Operational Details: description of services, number of members, scope of operations;

- (v) Financial Data: bank account details for receipt of Donations, subscription payment details, PayPal/Venmo or equivalent account information;
- (vi) Verification Data: organizational registration certificates, identification of legal representative, proof of registered office; and
- (vii) Donation Records: history of Donations received and distribution of funds.

3.2.2 Purpose of Collection:

- (i) to verify legitimacy and legal standing of the organization;
- (ii) to facilitate receipt and distribution of Donations from ProdigyCard sales;
- (iii) to enable subscription-based access to Platform features and analytics;
- (iv) to provide relevant communications, industry updates, and opportunities;
- (v) to comply with applicable AML, tax, and financial reporting obligations; and
- (vi) to enable networking and collaboration opportunities with student-athletes.

3.2.3 Personal Data Sharing:

- (i) business name and sport affiliation may be publicly listed as Donation beneficiaries or partners;
- (ii) financial data is shared with Payment Processors for payouts and subscription processing (if not already obtained by Payment Processors themselves during the KYC and AML verification);
- (iii) verification documents may be disclosed to regulators where legally required;
- (iv) contact information may be shared with student-athletes for collaboration with prior consent;
- (v) aggregated organizational data may be used for analytics and reporting.

3.3 Industry (Combined User Category)

This category includes scouts, agents, brands' representatives, coaches and similar industry professionals.

3.3.1 Personal Data Collected:

- (i) Professional Information: name of business/organization, business address, type of profession, sport/activity affiliation;
- (ii) Contact Data: first name, last name, verified email, verified phone number;
- (iii) Digital Presence: professional website, optional social media links;
- (iv) Business Details: description of services, client base, registration identification details;
- (v) Credentials: certifications, affiliations, licenses, professional standing; and
- (vi) Interaction Data: records of scouting reports, communications, comments, and engagement with other Users.

3.3.2 Purpose of Collection:

- (i) to verify professional identity and legitimacy;
- (ii) to enable networking and collaboration opportunities with student-athletes and other Users;
- (iii) to provide insights and analytics on performance and engagement;
- (iv) to ensure integrity and professional standards within the Platform;
- (v) to enable targeted communication about relevant opportunities.

3.3.3 Personal Data Sharing:

- (i) contact data may be shared with student-athletes or Guardians for collaboration, subject to explicit consent;
- (ii) professional credentials may be displayed to establish credibility; and
- (iii) interaction history may be used for analytics and service improvements.

3.4 Collectors (Combined User Category)

This category includes donors, investors and fans.

3.4.1 Personal Data Collected:

- (i) Contact Data: name, email address;
- (ii) Financial Data: Donation amounts, payment methods, transaction history;
- (iii) Preferences: preferred athletes, causes, or organizations to support; and
- (iv) Engagement Data: interaction history and usage patterns.

3.4.2 Purpose of Collection:

- (i) to process Donations and in-app purchases;
- (ii) to provide receipts and transaction confirmations;
- (iii) to communicate regarding Donations and their impact;
- (iv) to personalize experience and suggest relevant athletes or causes;
and
- (v) to facilitate donor recognition and acknowledgment systems.

3.4.3 Personal Data Sharing:

- (i) financial data is shared with Payment Processors for transaction execution (if not already obtained by Payment Processors themselves during the KYC and AML verification);
- (ii) Donation information (excluding personal financial details) may be shared with beneficiaries for acknowledgment; and
- (iii) aggregated donor data may be used for analytics and reporting.

3.5 Visitors

3.5.1 Personal Data Collected:

- (i) Usage Data: referred to in Section 2.1.7; and
- (ii) Cookie Data: referred to in Article 4.

3.5.2 Purpose of Collection:

- (i) to analyze traffic and usage behavior;
- (ii) to improve Platform functionality and security; and
- (iii) to provide essential services and maintain User session integrity.

3.5.3 Personal Data Sharing:

Aggregated, anonymized data may be shared with analytics providers.

3.6 Admin (ProdigyChain Internal Accounts)

3.6.1 Personal Data Collected:

- (i) Comprehensive User Data: full registration details, behavior data, and transaction history across all categories;
- (ii) Platform Analytics: ProdigyCard creation, transfers, User engagement metrics, and financial performance data;
- (iii) Compliance Records: GDPR and cookie preferences, consent logs, and audit trails; and

- (iv) System Data: platform performance metrics, security logs, error reports.

3.6.2 Purpose of Collection:

- (i) to monitor, manage, and improve Platform performance;
- (ii) to ensure compliance with GDPR, AML, and other regulatory obligations;
- (iii) to generate analytics, insights, and business reports;
- (iv) to manage content, including ProdigyCards, within the ProdigyVault; and
- (v) to provide technical and customer support.

3.6.3 Personal Data Sharing:

- (i) primarily for internal use within ProdigyChain and its affiliates;
- (ii) aggregated and anonymized data may be shared with analytics providers;
- (iii) transaction details may be shared with financial regulators or tax authorities as required by law; and
- (iv) system credentials are visible to Users during marketplace transactions.

All admin-collected data is retained for operational, compliance, and regulatory purposes, consistent with the retention periods set out in Section 2.6, Article 7 of this Policy and in the Appendix 1 to this Policy.

4 TRACKING TECHNOLOGIES AND COOKIES

We use cookies and similar tracking technologies to monitor activity on the Platform and to store certain information. Tracking technologies include browser cookies, Flash cookies, web beacons, pixel tags, and scripts. These technologies help us to collect and analyze information, to improve the Platform, and to deliver a more personalized user experience.

4.1 Cookies

A cookie is a small file that is stored on your device. You may configure your browser to refuse all cookies or to indicate when a cookie is being sent. Please note that if you refuse cookies, certain features of the Platform may not function properly. Unless you have modified your browser settings to refuse cookies, the Platform will use cookies.

4.1.1 Types of Cookies Used:

- (i) session Cookies: deleted once you close your browser; and

- (ii) persistent Cookies: remain stored on your device until deleted manually or by your browser after the expiry period.

4.2 Flash Cookies

Certain features of the Platform may use local stored objects (commonly known as “**Flash cookies**”) to collect and store information about your preferences or activity. Flash cookies are not managed through the same browser settings as browser cookies and may require separate management.

4.3 Web Beacons

Sections of the Platform and certain communications from us may include small electronic files known as web beacons (also referred to as clear gifs, pixel tags, or single-pixel gifs). Web beacons allow us to count Users who visit specific pages or open an email, and to generate related statistics (for example, tracking the popularity of certain content, verifying system integrity, or determining email engagement rates).

4.4 Purposes of Cookies and Tracking Technologies

- 4.4.1 necessary / essential Cookies are session Cookies that are Administered by us. Session Cookies are essential to provide you with the services available on the Platform and to enable use of certain features. They authenticate users, prevent fraudulent use of accounts, and are strictly necessary to deliver the services you request;
- 4.4.2 acceptance Cookies are persistent Cookies that are administered by us. Persistent Cookies record whether you have accepted the use of Cookies on the Platform, ensuring compliance with cookie consent requirements under applicable law;
- 4.4.3 functionality Cookies are persistent Cookies that are administered by us. Functionality Cookies enable the Platform to remember your choices, such as login credentials, language preferences, and other customizations, thereby providing you with a more personalized experience and avoiding repetitive entry of preferences;
- 4.4.4 analytics and performance Cookies (if used) are persistent Cookies that are administered by Service Providers (e.g., analytics providers). Analytics and performance Cookies collect aggregated information about how the Platform is used, allowing us to analyze performance, identify errors, and improve functionality; and
- 4.4.5 marketing and targeting Cookies (if consented) are persistent Cookies that are administered by us and/or third-party partners.

Marketing and targeting Cookies track your browsing activity to deliver relevant advertising and promotional messages, subject to your prior consent in accordance with GDPR and ePrivacy requirements.

4.5 Cookie Management

You may configure or withdraw your consent to non-essential cookies at any time via your browser settings or through the cookie consent banner provided on the Platform. Essential cookies cannot be disabled as they are strictly necessary for the operation of the Platform.

5 HOW WE USE AND PROCESS PERSONAL DATA

In addition to the general purposes of processing described in Section 2.3 of this Policy, we may use and process Personal Data for the following:

5.1 Provision and Maintenance of the Platform

To operate, secure, and improve the Platform, including monitoring usage, diagnosing technical issues, and ensuring functionality.

5.2 Account Management

To register, authenticate, and administer your Account, and to provide access to features available to registered Users.

5.3 Contract Performance

To develop, execute, and fulfill contractual obligations entered into with Users, including subscription services, acquisition of ProdigyCards, NIL monetization, and Donations.

5.4 Communications

To contact you by email, telephone, SMS, in-app notifications, or other channels regarding Platform updates, security alerts, and service-related information.

5.5 Marketing and Promotional Purposes

To provide you with news, special offers, and general information about products, services, or events offered by us or its partners that are similar to those you have previously purchased or requested, unless you have opted out of receiving such communications. Marketing communications will only be sent in compliance with applicable data protection and ePrivacy requirements, and subject to your prior consent where required.

5.6 User Requests and Support

To respond to, manage, and resolve your requests, inquiries, or complaints.

5.7 Business Transactions

To evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other corporate transaction, including the sale or transfer of our assets, where Personal Data may form part of the transferred assets.

5.8 Analytics and Improvements

To conduct data analysis, identify usage trends, measure the effectiveness of promotional campaigns, and evaluate and improve the Platform, products, services, and overall User experience.

5.9 Minor Protection

To ensure compliance with applicable laws regarding Minors, to verify Guardian consent, and to facilitate proper Guardian oversight of Minor Users' activities on the Platform.

6 SHARING OF PERSONAL DATA

We may share Personal Data under the following circumstances:

- 6.1 **with Service Providers:** to enable monitoring and analysis of Platform use, to facilitate communications, and to process payments;
- 6.2 **with affiliates:** with our parent and subsidiary entities, provided that such affiliates are bound by this Policy and equivalent data protection obligations;
- 6.3 **with business partners:** with carefully selected partners in order to provide you with relevant products, services, or promotional offerings;
- 6.4 **with other Users:** when you voluntarily share information or interact within the public areas of the Platform, such data may be visible to all Users and publicly disseminated outside the Platform. For Minors, contact information is never made publicly available;
- 6.5 **with consent:** for any other purpose not described above, provided that you (and in the case of Minors, your Guardian) have given explicit consent.

For disclosures required by law or in special circumstances, see Article 9 of this Policy.

7 RETENTION OF PERSONAL DATA

7.1 General Retention Principle

We will retain Personal Data only for as long as necessary to fulfill the purposes set out in this Policy, or as otherwise required to comply with applicable legal, regulatory, accounting, or reporting obligations. Personal Data may also be retained as necessary to establish, exercise, or defend legal claims. The following shall apply:

7.2 Statutory and Contractual Obligations

- 7.2.1 Account and registration data are retained for five (5) years after closure;
- 7.2.2 Donation and beneficiary records are retained for ten (10) years after date of transaction;
- 7.2.3 Guardian consent records are retained until the Minor reaches 18 years of age, plus five (5) years;
- 7.2.4 KYC/AML and financial data are retained for ten (10) years, or longer where legally mandated;
- 7.2.5 communications are retained for five (5) years for accountability purposes;
- 7.2.6 Usage Data is generally retained for two (2) years, unless required longer for security or compliance;
- 7.2.7 NIL/ProdigyCard data is retained for the duration of the Account and up to five (5) years thereafter;
- 7.2.8 system and security logs data are retained from two (2) to five (5) years, depending on nature of the log and security requirements; and
- 7.2.9 employment/contractor data are retained for the duration of employment/contractual relationship and statutory retention thereafter.

7.3 Special Retention Considerations for Minors

- 7.3.1 **Guardian consent records:** retained until the Minor reaches 18 years of age o, plus the applicable statutory limitation period for claims;
- 7.3.2 **Financial transaction records:** retained in accordance with financial and AML regulations, generally for a minimum of ten (10) years; and
- 7.3.3 **Communications with Guardians:** retained for accountability, transparency, and compliance purposes, generally for a minimum of five (5) years after the relevant transaction or communication.

7.4 Deletion or Anonymization

Upon expiration of the applicable retention period, Personal Data will either be securely deleted, anonymized, or aggregated so that it can no longer be linked to an identified or identifiable User. Where deletion is not technically feasible, we will implement appropriate safeguards to ensure the data is securely isolated and protected from further processing.

Please see the detailed overview in Appendix 1.

8 TRANSFER OF PERSONAL DATA

8.1 General Principle

Personal Data may be processed at our operating offices and in any other locations where we, our affiliates, or Service Providers are situated. This may involve the transfer of Personal Data to jurisdictions outside your state, province, country, or other governmental jurisdiction where data protection laws may not provide the same level of protection as in your home jurisdiction.

8.2 Legal Framework for International Transfers

Where Personal Data is transferred outside the European Economic Area (“EEA”) or other jurisdictions with equivalent data protection regimes, we ensure that such transfers are conducted in compliance with applicable law, including:

- 8.2.1 **Adequacy decisions:** transfers to jurisdictions recognized by the European Commission as providing adequate protection;
- 8.2.2 **Standard Contractual Clauses (SCCs):** EU-approved contractual provisions obligating recipients to safeguard Personal Data;
- 8.2.3 **Other appropriate safeguards:** binding corporate rules, codes of conduct, or certifications recognized under GDPR.

8.3 User Consent

By consenting to this Policy and submitting Personal Data through the Platform, you acknowledge and agree that your Personal Data may be transferred internationally in accordance with this Policy. Consent may be withdrawn at any time; however, this may limit your ability to use certain features of the Platform.

8.4 Safeguards and Security Measures

We take all steps reasonably necessary to ensure that Personal Data is handled securely and in accordance with this Policy. No transfer of Personal Data will take place to an organization or jurisdiction unless appropriate safeguards are in place, including contractual obligations to ensure confidentiality, integrity, and security of the data.

8.5 Enhanced Protections for Minors

- 8.5.1 enhanced encryption and security protocols for transmission and storage;
- 8.5.2 strict contractual obligations with international Service Providers requiring compliance with GDPR or stricter standards;

- 8.5.3 regular audits of international data handling practices, focusing on Minor-specific safeguards;
- 8.5.4 application of the most protective applicable privacy regime, ensuring that where multiple laws apply, the stricter standard governs; and
- 8.5.5 Guardian notification of international transfers where feasible and appropriate.

9 DISCLOSURE OF PERSONAL DATA

9.1 Business Transactions

If we are involved in a merger, acquisition, divestiture, restructuring, reorganization, dissolution, or sale of assets, Personal Data may be transferred as part of the transaction. In such cases, we will provide advance notice, where feasible, before Personal Data becomes subject to a different privacy policy. The receiving entity will be required to process the data in accordance with this Policy or provide equivalent protections.

9.2 Law Enforcement

Under certain circumstances, we may be legally obligated to disclose Personal Data in response to valid requests by public authorities, such as courts, regulators, supervisory authorities, or government agencies.

9.3 Other Legal Requirements

We may disclose Personal Data where it has a good faith belief that such disclosure is necessary to:

- 9.3.1 comply with a legal or regulatory obligation;
- 9.3.2 protect and defend the rights, property, or safety of ProdigyChain, its affiliates, or its Users;
- 9.3.3 prevent, detect, or investigate potential wrongdoing in connection with the Platform;
- 9.3.4 protect the personal safety of Users of the Platform or the general public; or
- 9.3.5 defend against legal claims or protect against legal liability.

9.4 Special Protections for Minors

- 9.4.1 **Guardian notification:** Guardians must be notified of any legal disclosure requests, unless prohibited by law or court order;
- 9.4.2 **Minimization:** disclosures are strictly limited to the minimum data necessary to comply with the legal request;

- 9.4.3 **Proportionality review:** we will challenge requests that are overly broad or disproportionate, particularly where Minor data is involved;
- 9.4.4 **Record-keeping:** all disclosures involving Minor data are documented, and records are made available to Guardians when legally permissible;
- 9.4.5 **Enhanced security:** Minor-related disclosures are subject to heightened safeguards, including encryption and restricted personnel access.

10 SECURITY OF PERSONAL DATA

10.1 General Security Measures

The security of your Personal Data is of paramount importance to us. While no method of transmission over the internet or method of electronic storage can be guaranteed to be 100% secure, we implement appropriate technical and organizational measures designed to ensure a level of security appropriate to the risk, including:

- 10.1.1 encryption and pseudonymization of Personal Data;
- 10.1.2 multi-factor authentication for access to sensitive systems;
- 10.1.3 firewalls, intrusion detection, and prevention systems;
- 10.1.4 secure development and deployment practices;
- 10.1.5 staff training and access controls based on the principle of least privilege;
- 10.1.6 regular penetration testing and vulnerability assessments; and
- 10.1.7 business continuity and disaster recovery planning.

These measures are implemented in line with Article 32 GDPR, which requires controllers and processors to ensure a level of security appropriate to the risk, taking into account the state of the art, implementation costs, and the nature, scope, context, and purposes of processing.

These measures are continuously reviewed and updated in line with technological developments and industry standards.

10.2 Limitations

Despite these efforts, no security measure can provide absolute protection against all threats. Users acknowledge that residual risk remains inherent in all online activities.

10.3 Enhanced Security Measures for Minors

- 10.3.1 **Additional encryption:** all Minor-related Personal Data is encrypted both in transit and at rest using advanced cryptographic protocols;
- 10.3.2 **Restricted access:** access to Minor-related data is strictly limited to authorized personnel with enhanced clearance, and such access is logged and monitored;
- 10.3.3 **Enhanced monitoring and logging:** all access to Minor User accounts is monitored in real time, with automated alerts for suspicious or unauthorized activities;
- 10.3.4 **Regular security audits:** periodic audits specifically targeted at Minor-related processing activities to assess the effectiveness of implemented safeguards; and
- 10.3.5 **Incident notification protocols:** Guardians are notified without undue delay in the event of any data breach or security incident affecting a Minor's Personal Data, consistent with GDPR Articles 33 and 34.

11 YOUR PERSONAL DATA PROTECTION RIGHTS

11.1 Rights under the GDPR (European Economic Area)

If you are located in the European Economic Area (EEA), we will take all reasonable steps to enable you to exercise your rights under the GDPR. Subject to the conditions set out in applicable law, you have the following rights:

- 11.1.1 **Right of access:** to obtain confirmation as to whether your Personal Data is being processed, and, where applicable, to receive a copy of such data together with additional information about the processing;
- 11.1.2 **Right to rectification:** to request the correction of inaccurate Personal Data and the completion of incomplete Personal Data;
- 11.1.3 **Right to Erasure (“Right to be Forgotten”):** to request the deletion of your Personal Data where grounds for erasure apply under GDPR, such as withdrawal of consent, unlawful processing, or where data is no longer necessary;
- 11.1.4 **Right to Restrict Processing:** to request that the processing of your Personal Data be restricted in certain cases (e.g., where accuracy is contested or processing is unlawful);
- 11.1.5 **Right to object:** to object to processing carried out on the basis of legitimate interests or for direct marketing purposes; and
- 11.1.6 **Right to data portability:** to receive Personal Data you have provided in a structured, commonly used, and machine-readable format, and to have that data transmitted to another controller, where technically feasible.

11.2 Special Rights for Minors and Guardians under the GDPR:

- 11.2.1 Guardians will exercise all GDPR rights on behalf of Minor Users;
- 11.2.2 An enhanced right to erasure applies once a Minor reaches 18 years of age of majority, allowing the User or Guardian to request deletion of data collected during minority;
- 11.2.3 Guardians have the right to obtain copies of all records of processing activities involving the Minor; and
- 11.2.4 Guardians and Minors have the right to object to any processing that is not strictly necessary for the operation of the Platform.

11.3 How to Exercise Your Rights

Requests to exercise your rights may be submitted by contacting us at info@prodigychain.com. We may require reasonable verification of your identity (and in the case of Minors, verification of Guardian authority) before fulfilling any request. Responses will be provided within the timeframes required by applicable law.

12 CHILDREN'S PRIVACY ENHANCED PROTECTIONS

12.1 Children Under the Age of 14

The Platform is not directed to children under the age of fourteen (14). We do not knowingly collect or process Personal Data from children under 14 years of age. If you become aware that a child under 13 years of age has provided Personal Data to us without appropriate parental consent, you must notify us immediately at info@prodigy-chain.ai. If we become aware that it has inadvertently collected Personal Data from a child under 13 years of age without parental consent, such data will be promptly deleted from our systems, and all associated processing activities will cease.

12.2 Enhanced Protection Framework for Minors

We apply a comprehensive framework of enhanced safeguards to protect Minor, including the following:

12.3 Onboarding Process

- 12.3.1 **Age verification:** robust procedures to verify the age of all new Users during account creation;
- 12.3.2 **Guardian identification:** verification of the identity of the parent or legal Guardian;
- 12.3.3 **Consent documentation:** comprehensive consent forms clearly explaining Platform activities, rights, and responsibilities;

12.3.4 **Financial authorization:** Guardian approval required for all financial transactions, verified through integrated payment processing (e.g., Stripe); and

12.3.5 **Ongoing oversight:** mechanisms enabling Guardians to maintain continuous oversight of Minors' accounts.

12.4 Operational Protections

12.4.1 **Data minimization:** collection limited strictly to information essential for providing Platform services;

12.4.2 **Privacy by design and default:** all Minor accounts are configured with the highest privacy settings by default;

12.4.3 **Communication controls:** copies of all communications are provided to verified Guardians, and Minors are restricted from engaging in unsupervised communications;

12.4.4 **Transaction oversight:** Guardian authorization required for all financial operations, including ProdigyCard transactions and Donations; and

12.4.5 **Regular reviews:** periodic compliance and safety reviews of Minor accounts conducted by us.

12.5 Legal Compliance

12.5.1 **Multi-jurisdictional standards:** compliance with GDPR Article 8, and other relevant local laws;

12.5.2 **Integrated financial safeguards:** use of Payment Processors with specific protections for transactions involving Minors;

12.5.3 **Documentation:** maintenance of detailed records of all Guardian consents, financial authorizations, and Minor-related activities; and

12.5.4 **Audit trail:** creation and preservation of complete audit trails evidencing compliance and Guardian oversight.

13 CONTACT INFORMATION

If you have any questions about this Policy, the processing of your Personal Data, or if you wish to exercise your data protection rights, you may contact us at:

By email: info@prodigy-chain.ai

By visiting our contact page: www.prodigy-chain.ai

By mail: ProdigyChain, j.s.a., Karpatská 7, 911 01 Trenčín, Slovak Republic

Guardians of Minors can contact us using the above methods with “*Guardian Inquiry*” in the subject line for priority handling of Minor-related matters.

14 CHANGES TO THIS POLICY

We may amend or update this Policy from time to time to reflect changes in our practices, legal requirements, or other operational reasons. Any changes will be effective as of the “Last Updated” date indicated at the top of this Policy.

For material changes, we will provide appropriate notice, which may include posting the updated Policy on the Platform, sending notices by email, and/or displaying in-app notifications, as required by applicable law.

Where changes to this Policy affect the rights or obligations of Minors, we will provide enhanced notification, including:

- 14.1.1 direct notification to all verified Guardians;
- 14.1.2 a clear explanation of how the changes affect Minors and Minor-related processing;
- 14.1.3 an opportunity for Guardians to review the changes and re-consent to the continued processing of the Minor’s Personal Data and continued use of the Platform; and
- 14.1.4 provision of a reasonable grace period during which Guardians may withdraw consent and/or disable the Minor’s account without penalty.

We may specifically require Guardians to provide consent to the updated Policy (or to specified processing activities covered by the updated Policy) before further use of the Platform by the Minor is permitted. Where consent is the relevant legal basis for a processing activity, failure to provide (or maintain) consent may result in suspension or limitation of the Minor’s access to the affected features. For processing activities based on other legal grounds (e.g., contract performance or legal obligation), we will inform Guardians of the available options (such as the right to object, account closure, or deletion requests) in accordance with applicable law.

You are encouraged to review this Policy periodically to stay informed about how we collect, process, store, and disclose Personal Data. Continued use of the Platform after the effective date of any changes constitutes acceptance of the revised Policy.

15 LEGAL BASES FOR PROCESSING (GDPR)

We process Personal Data only where a valid legal basis exists under Article 6 of the GDPR. Depending on the context, one or more of the following legal bases may apply:

15.1 Performance of a Contract (Article 6(1)(b) GDPR)

Processing is lawful where it is necessary for the performance of a contract to which the User is a party, or to take steps at the request of the User prior to entering into a contract. This includes, for example:

- 15.1.1 registering and managing your Account;
- 15.1.2 enabling the creation, minting, and transfer of ProdigyCards;
- 15.1.3 processing payments, subscriptions, and Donations;
- 15.1.4 providing access to educational resources and networking opportunities; and
- 15.1.5 providing customer support and responding to User requests.

15.2 Compliance with Legal Obligations (Article 6(1)(c) GDPR)

Processing is lawful where it is necessary to comply with obligations under applicable law. This includes:

- 15.2.1 AML and KYC requirements;
- 15.2.2 tax and accounting obligations;
- 15.2.3 record-keeping requirements under Slovak, EU, and U.S. law; and
- 15.2.4 responding to lawful requests from courts, regulators, or law enforcement authorities.

15.3 Legitimate Interests (Article 6(1)(f) GDPR)

Processing may be based on our legitimate interests, provided that such interests are not overridden by your fundamental rights and freedoms. Legitimate interests include:

- 15.3.1 ensuring the safety, integrity, and security of the Platform;
- 15.3.2 preventing fraud, abuse, and misuse of services;
- 15.3.3 conducting analytics and improving Platform functionality;
- 15.3.4 developing and enhancing services and features; and
- 15.3.5 protecting and defending ProdigyChain's rights, property, and interests.

15.4 Consent (Article 6(1)(a) GDPR)

Processing is lawful where you (or, in the case of Minors, your Guardian) have given explicit consent for a specific purpose. Consent may be sought for:

- 15.4.1 receiving marketing communications, newsletters, or promotional offers;
- 15.4.2 the sharing of certain Personal Data with business partners or third parties;
- 15.4.3 the use of cookies and similar technologies for analytics or marketing (where not strictly necessary); and

15.4.4 participation in optional features of the Platform.

Consent can be withdrawn at any time, without affecting the lawfulness of processing carried out prior to withdrawal. Withdrawal may limit or restrict access to certain Platform functionalities that depend on consent.

Where processing involves special categories of Personal Data as defined in Article 9 of the GDPR, we will only carry out such processing where one of the conditions in Article 9(2) applies, including explicit consent of the User (or, in the case of Minors, the verified Guardian).

15.5 Special Considerations for Minors

For Minors, consent must be obtained from a verified Guardian before Personal Data is processed for purposes requiring consent. Guardians retain the right to withdraw consent at any time. Where processing is based on other legal grounds (such as contract performance or legal obligation), Guardians will be informed of their rights, including the right to object or request deletion of data, consistent with applicable law.

16 DATA PROTECTION OFFICER AND PRIVACY CONTACT

We have appointed a Data Protection Officer (“DPO”) to oversee compliance with this Policy and applicable data protection laws. The DPO also serves as the primary point of contact for all questions, requests, and concerns relating to the processing of Personal Data.

Designated Data Protection Officer:

Email: info@prodigy-chain.ai

You may contact the DPO or at the above email address for any inquiries regarding this Policy, the processing of your Personal Data, or to exercise your rights under applicable data protection law.

Guardians of Minors may also contact the DPO directly, using “*Guardian Inquiry*” in the subject line, for priority handling of Minor-related matters.

17 AUTOMATED DECISION-MAKING AND PROFILING

We may use automated processing, including limited profiling, in connection with certain Platform features such as ProdigyRankings, scholarship matching, or analytics designed to enhance User experience. Automated decision-making will never:

- 17.1.1 produce legal or similarly significant effects without appropriate human oversight;
- 17.1.2 involve the use of special categories of Personal Data (e.g., health, biometric, or political data) without explicit consent; or

17.1.3 limit the rights of Minors or Guardians to object, review, or contest any decision.

User Rights under GDPR Article 22:

17.1.4 You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning You or similarly significantly affects You;

17.1.5 You have the right to obtain human intervention, to express Your point of view, and to contest any such decision; and

17.1.6 Guardians may exercise these rights on behalf of Minors.

We will ensure transparency by clearly explaining when automated decision-making is applied and the logic involved, as well as the significance and potential consequences of such processing.

17. SUPERVISORY AUTHORITY AND COMPLAINTS

If you believe that your data protection rights have been infringed, you have the right to lodge a complaint with a supervisory authority.

The competent supervisory authority for ProdigyChain is:

Úrad na ochranu osobných údajov Slovenskej republiky (*Office for Personal Data Protection of the Slovak Republic*)

Budova Park one

Námestie 1.mája 18

811 06 Bratislava

Slovenská republika

Website: <https://dataprotection.gov.sk>

You also have the right to lodge a complaint with the supervisory authority of your habitual residence, place of work, or place of the alleged infringement, within the European Economic Area (EEA).

We would, however, appreciate the opportunity to address your concerns before you approach a supervisory authority and therefore encourages you to contact the DPO or Team in the first instance.

DMCA/ EU Copyright Notice Procedure. If you believe your copyrighted material has been used or shared on our Platform without authorization, please refer to the Terms, Article 13, section (ix) and (x).

APPENDIX 1 DATA RETENTION SCHEDULE

We retain Personal Data only for as long as necessary to fulfill the purposes described in this Policy or to comply with legal, regulatory, or contractual obligations. Upon

expiration of the retention period, Personal Data will be securely deleted, anonymized, or aggregated.

The following table provides an overview of retention periods by category of data:

Category of Personal Data	Retention Period	Legal/Operational Basis
Account and Registration Data	For the duration of the User's account and up to 5 years after closure	Contract performance; limitation periods for contractual claims
Guardian Consent Records (Minors)	Until the Minor reaches 18 years of age + 5 years	Compliance with GDPR Art. 8; accountability; limitation periods
Financial and Transaction Data	10 years from transaction date or termination of relationship	Tax and accounting laws; AML regulations
KYC/AML Verification Data	Minimum 10 years from transaction date or termination of relationship	AML and counter-terrorist financing legislation
ProdigyCard and NIL Data	For the duration of the User's account and up to 5 years thereafter	Contract performance; limitation periods; audit and accountability
Donations and Beneficiary Records	10 years from the date of transaction	Accounting, AML, and charity law compliance
Communications with Users/Guardians	Minimum 5 years after resolution of the relevant inquiry or transaction	Accountability; audit trail; safeguarding Minors
Usage and Analytics Data	Generally 2 years, unless required longer for security, functionality, or legal obligations	Legitimate interests; system integrity; fraud prevention
System and Security Logs	2 to 5 years, depending on the nature of the log and security requirements	Legitimate interests; GDPR Art. 32 (security of processing)
Employment/Contractor Data (if any)	For the duration of the employment/contractual relationship and statutory retention thereafter	Labor law; tax and social security regulations

APPENDIX 2

DATA PROTECTION IMPACT ASSESSMENT (DPIA) TEMPLATE

This template is provided to facilitate the systematic assessment of processing activities involving Personal Data, particularly those that may result in high risks to the rights and freedoms of natural persons, including Minor Users. We will use this DPIA template to evaluate new projects, features, or significant changes to existing processing activities.

1. **Description of Processing Activity:** Provide a detailed overview of the processing operation, including the purpose, scope, and context.
2. **Categories of Data Subjects:** Identify the groups of data subjects affected (e.g., Student Athletes, Minors, Guardians, Donors, etc.).
3. **Categories of Personal Data:** Specify the types of Personal Data collected and processed (e.g., identification data, financial data, NIL data).
4. **Purpose and Legal Basis:** Describe the purposes of processing and identify the applicable legal bases under GDPR Article 6 (and Article 9 if special categories of data are involved).
5. **Necessity and Proportionality:** Assess why the processing is necessary for the stated purposes and how it is proportionate.
6. **Risks to Data Subjects:** Identify potential risks to the rights and freedoms of data subjects (e.g., unauthorized access, loss of confidentiality, discrimination, misuse of Minor data).
7. **Safeguards and Mitigation Measures:** Detail the technical and organizational measures implemented to address identified risks (e.g., encryption, pseudonymization, access controls, Guardian oversight).
8. **Involvement of Stakeholders:** Document consultations with Guardians, Users, or supervisory authorities where relevant.
9. **Residual Risks and Balancing Test:** Evaluate whether any residual risks remain and whether they are justified by the benefits of processing.
10. **Review and Monitoring:** Establish procedures for ongoing review of the DPIA and updates when processing activities change.

The DPIA must be signed and approved by the Data Protection Officer (DPO) before the commencement of the processing activity.

Disclaimer. This Data Protection Impact Assessment (“DPIA”) template is provided as an internal compliance tool for us. It is intended solely to support the identification, assessment, and mitigation of data protection risks in accordance with GDPR and other applicable laws. This template does not form part of the Policy as a contractual undertaking and does not create any legal rights or obligations for Users of the Platform. Nothing in this Appendix 2 shall be construed as a binding representation, warranty, or guarantee to Users regarding the outcome of any specific DPIA carried out by us.