

1. Data Controller

This Privacy Policy describes how Pladinum Group SL processes personal data in connection with its website(s), customer portal, infrastructure, and the products and services it offers.

The data controller for the purposes of the General Data Protection Regulation (EU) 2016/679 ("GDPR") is:

Pladinum Group SL

Avenida de Manolete 3a
29660 Marbella, Malaga (ES)
CIF: ESB72758436

Data Protection Contact: privacy@pladinum.com

Telephone: +34 697 9898 40

Customer Portal: my.pladinum.com

In certain service contexts, Pladinum acts as a data processor on behalf of the Customer (the data controller). The respective roles and obligations are defined in the Data Processing Agreement (DPA) concluded between Pladinum and the Customer in accordance with Article 28 GDPR.

2. Scope and Applicability

2.1 This Privacy Policy applies to all individuals whose personal data is processed by Pladinum, including current, former, and prospective customers, website visitors, newsletter subscribers, support contacts, and any other persons interacting with Pladinum's services.

2.2 This policy should be read together with our General Terms and Conditions, Cookie Policy, Acceptable Use Policy, and any applicable service-specific agreements.

2.3 Applicable Legislation. Pladinum processes personal data in compliance with the General Data Protection Regulation (EU) 2016/679, the Spanish Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), the ePrivacy Directive (2002/58/EC), and any other applicable EU or national data protection legislation.

3. Key Definitions

"Personal Data" means any information relating to an identified or identifiable natural person ("data subject"), including name, email address, IP address, identification numbers, location data, online identifiers, and any factor specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

"Processing" means any operation performed on personal data, whether automated or not, including collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, alignment, restriction, erasure, or destruction.

"Data Controller" means the entity that determines the purposes and means of the processing of personal data.

"Data Processor" means the entity that processes personal data on behalf of the controller.

"Consent" means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they signify agreement to the processing of their personal data.

4. Personal Data We Collect

Pladinum collects personal data through various channels depending on how you interact with us. The categories of data collected include:

4.1 Data You Provide Directly

Account Registration: Name, email address, postal address, telephone number, company name, VAT identification number, and login credentials.

Service Orders: Billing information, payment method details, domain name registration data (including WHOIS information), and service configuration preferences.

Support Interactions: Information provided through support tickets, live chat (Chatwoot), email correspondence, and telephone calls.

Newsletter Subscription: Email address and, optionally, name and company details.

Contact Forms: Name, email address, and the content of your inquiry.

4.2 Data Collected Automatically

Technical Data: IP address, browser type and version, operating system, device type, screen resolution, referring URL, and pages visited.

Usage Data: Date and time of access, clickstream data, session duration, features used, and interaction patterns.

Server Logs: Access logs, error logs, and security event logs generated in connection with hosting and infrastructure services.

Cookies and Trackers: Data collected through cookies and similar technologies, as described in detail in our Cookie Policy.

4.3 Data from Third Parties

Domain Registries: Information received from domain registries (e.g., via OpenProvider) in connection with domain registration, transfer, or dispute resolution.

Payment Processors: Transaction confirmation data received from payment service providers.

Publicly Available Sources: Information from public WHOIS databases or business registries, where relevant to the provision of Services.

4.4 Domain Name Registration Data

Where you register, transfer, or renew a domain name through Pladinum, the following applies in addition to the above.

Purposes. Registration data is collected to register and administer the domain name, to comply with the policies of ICANN and of the registry responsible for the extension, and to meet Pladinum's obligations to the sponsoring registrar.

Recipients. Registration data is transmitted to the sponsoring registrar, the registry operator responsible for the extension, ICANN where applicable, and an escrow agent appointed under the ICANN Registrar Accreditation Agreement. Certain data may be published in public WHOIS or RDAP directories in accordance with registry policy.

Obligatory and voluntary data. The data fields required vary by extension and are indicated at the point of collection. Fields not marked as required are voluntary.

Access and rectification. You may access and correct your registration data at any time through the customer portal. You are required to keep it accurate and to correct it within seven (7) days of any change. Failure to respond within fifteen (15) days to a request to verify contact details is a material breach and grounds for suspension of the domain name.

Retention. Registration data is retained in accordance with the ICANN Data Retention Specification and the rules of the relevant registry. Pladinum may be required to disclose this data within seven (7) days of a request made under those specifications.

5. Purposes and Legal Bases for Processing

Pladinum processes personal data only where there is a valid legal basis under Article 6 GDPR. The following table maps each processing purpose to its lawful basis:

Processing Purpose	Legal Basis (Art. 6 GDPR)	Details
Account creation and management	Performance of contract (Art. 6(1)(b))	Necessary to set up and maintain your Account and deliver Services
Provision of hosting, domain, SSL, email, VPN, security, and backup services	Performance of contract (Art. 6(1)(b))	Required for the delivery of the specific Services ordered
Billing, invoicing, and payment processing	Performance of contract (Art. 6(1)(b))	Required to process payments and manage your subscription
Customer support and technical assistance	Performance of contract (Art. 6(1)(b))	Required to respond to inquiries and resolve issues
Security monitoring, fraud prevention, and abuse detection	Legitimate interest (Art. 6(1)(f))	Pladinum's legitimate interest in protecting its infrastructure, customers, and Services
Network and infrastructure monitoring	Legitimate interest (Art. 6(1)(f))	Ensuring stability, performance, and security of hosted environments
Compliance with legal obligations (tax, accounting, law enforcement)	Legal obligation (Art. 6(1)(c))	Required under Spanish and EU fiscal, accounting, and regulatory law
Marketing communications and newsletters	Consent (Art. 6(1)(a))	Only with your prior opt-in consent; you may withdraw at any time
Website analytics and performance improvement	Consent (Art. 6(1)(a)) / Legitimate interest (Art. 6(1)(f))	Analytics cookies require consent; aggregated analysis may rely on legitimate interest
Pre-contractual inquiries and quotations	Pre-contractual measures (Art. 6(1)(b))	Processing data you provide when requesting information about our Services
Dispute resolution and legal proceedings	Legitimate interest (Art. 6(1)(f)) / Legal obligation (Art. 6(1)(c))	Establishing, exercising, or defending legal claims
Product development, research, and trend analysis	Legitimate interest (Art. 6(1)(f))	Using anonymised or aggregated data to improve Services

Where processing is based on legitimate interest, Pladinum conducts a balancing test to ensure that its interests do not override the fundamental rights and freedoms of the data subject. You have the right to object to processing based on legitimate interest at any time (see Section 9).

6. Recipients and Third-Party Sharing

6.1 General Principle. Pladinum does not sell, rent, or trade personal data to third parties. Personal data is shared only where necessary to fulfil the purposes described in this policy, and always subject to appropriate safeguards.

6.2 Categories of Recipients

Infrastructure Partners: Leaseweb (dedicated server infrastructure), hosting and colocation services.

Domain and SSL Providers: OpenProvider, domain name registration, transfer, management, and SSL certificate issuance.

Backup and Disaster Recovery: Acronis, backup storage and disaster recovery processing.

GDPR Compliance Tooling: CookieFirst (Digital Data Solutions BV, Netherlands), cookie consent management.

Payment Processors: Stripe (Stripe Payments Europe, Ltd.), payment processing for transactions.

Analytics: Google Analytics (Google Ireland Limited), website usage analysis with IP anonymisation enabled.

Email Infrastructure: Pladinum operates its own mail and newsletter infrastructure; inbound and outbound email for hosted mailboxes is filtered through SpamExperts (email security filtering).

6.3 Legal and Regulatory Disclosures

Pladinum may disclose personal data to competent authorities (including law enforcement, tax authorities, and regulatory bodies) where required by law, court order, or in the context of a police or judicial investigation. Such disclosures are made on a confidential basis and limited to the minimum data necessary.

6.4 Affiliates and Successors

Pladinum may share personal data with affiliated companies or legal successors (e.g., in the context of a merger, acquisition, or restructuring) for the same purposes described in this policy. In such cases, the successor entity will be bound by equivalent data protection obligations.

6.5 Sub-Processors

All third-party service providers that process personal data on behalf of Pladinum are contractually bound by Data Processing Agreements in accordance with Article 28 GDPR. A current, versioned list of sub-processors is published on the Site. Customers may subscribe to be notified of additions or replacements in advance, in accordance with Section 6.3 of the Data Processing Agreement.

7. International Data Transfers

7.1 Pladinum primarily processes personal data within the European Economic Area (EEA). Where personal data is transferred to countries outside the EEA that do not benefit from an adequacy decision by the European Commission, Pladinum ensures that appropriate safeguards are in place.

7.2 Transfer Mechanisms. International transfers are safeguarded by one or more of the following mechanisms: (i) Standard Contractual Clauses (SCCs) approved by the European Commission (Commission Implementing Decision (EU) 2021/914); (ii) an adequacy decision by the European Commission (e.g., the EU-US Data Privacy Framework, where applicable); or (iii) binding corporate rules, where available.

7.3 Where Pladinum engages sub-processors located outside the EEA (e.g., Google LLC for analytics), the specific transfer mechanism and supplementary measures are documented in the relevant Data Processing Agreement.

7.4 You may request information about the safeguards applied to international transfers by contacting privacy@pladinum.com.

8. Data Retention

Pladinum retains personal data only for as long as necessary to fulfil the purposes for which it was collected, or as required by applicable law. The following retention periods apply:

Category of Data	Retention Period	Legal Basis for Retention
Account and service data	Duration of the contractual relationship + 30 days for data export	Contractual necessity
Billing, invoicing, and tax records	7 years after the end of the financial year in which the transaction occurred	Spanish tax and accounting obligations (Ley General Tributaria)
Data retained for legal claims and dispute resolution	Up to 10 years after the end of the contractual relationship	Limitation periods under Spanish civil law
Support tickets and correspondence	3 years after resolution	Legitimate interest in service quality and dispute prevention
Marketing consent records	Duration of consent + 3 years after withdrawal	Accountability obligations (Art. 5(2) GDPR)
Server and access logs (security)	12 months	Legitimate interest in security and incident investigation
Website analytics data	14 months (Google Analytics default)	Consent-based; configurable retention
Cookie consent preferences	12 months	ePrivacy compliance
Newsletter subscriber data	Until unsubscription + 30 days	Consent-based

Upon expiry of the applicable retention period, personal data is securely deleted or irreversibly anonymised. Where anonymised data is retained for statistical or research purposes, it can no longer be linked to an identifiable individual.

9. Your Rights Under GDPR

Under the GDPR and applicable national legislation, you have the following rights in relation to your personal data. These rights may be exercised free of charge by contacting privacy@pladinum.com or through the customer portal at my.pladinum.com.

9.1 Right of Access (Art. 15 GDPR). You have the right to obtain confirmation of whether Pladinum processes your personal data, to access that data, and to receive a copy thereof. You may also request information about the purposes, categories of data, recipients, retention periods, and the existence of automated decision-making.

9.2 Right to Rectification (Art. 16 GDPR). You have the right to request the correction of inaccurate personal data and the completion of incomplete personal data. You may update your data directly through the customer portal at my.pladinum.com.

9.3 Right to Erasure (Art. 17 GDPR). You have the right to request the deletion of your personal data where: (i) the data is no longer necessary for the purposes for which it was collected; (ii) you withdraw consent and no other legal basis exists; (iii) you object to processing and no overriding legitimate grounds exist; (iv) the data has been unlawfully processed; or (v) deletion is required to comply with a legal obligation. This right is subject to limitations where retention is required by law (e.g., tax and accounting records).

9.4 Right to Restriction of Processing (Art. 18 GDPR). You have the right to request the restriction of processing where: (i) you contest the accuracy of the data (restricted during verification); (ii) the processing is unlawful but you oppose erasure; (iii)

Pladinum no longer needs the data but you require it for legal claims; or (iv) you have objected to processing pending verification of legitimate grounds.

9.5 Right to Data Portability (Art. 20 GDPR). You have the right to receive your personal data in a structured, commonly used, and machine-readable format, and to request the direct transfer of that data to another controller, where technically feasible. This right applies to data processed on the basis of consent or contract and by automated means.

9.6 Right to Object (Art. 21 GDPR). You have the right to object, at any time, to the processing of your personal data based on legitimate interest (Art. 6(1)(f) GDPR), including profiling. Pladinum shall cease processing unless it demonstrates compelling legitimate grounds that override your interests, rights, and freedoms, or the processing is necessary for legal claims. Where personal data is processed for direct marketing purposes, you have an absolute right to object at any time.

9.7 Right to Withdraw Consent (Art. 7(3) GDPR). Where processing is based on consent, you may withdraw that consent at any time. Withdrawal does not affect the lawfulness of processing carried out prior to withdrawal. You may withdraw consent by: (i) clicking the unsubscribe link in marketing emails; (ii) adjusting cookie preferences via the CookieFirst consent banner; or (iii) contacting privacy@pladinum.com.

9.8 Right Not to Be Subject to Automated Decision-Making (Art. 22 GDPR). You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects you. Pladinum does not currently engage in solely automated decision-making that produces legal effects on data subjects.

9.9 Right to Lodge a Complaint. If you believe that Pladinum has processed your personal data in violation of applicable data protection law, you have the right to lodge a complaint with the competent supervisory authority. For Spain, this is the Agencia Española de Protección de Datos (AEPD), C/ Jorge Juan 6, 28001 Madrid, Spain (www.aepd.es).

Response Timeline. Pladinum shall respond to all data subject requests within one (1) month of receipt. This period may be extended by a further two (2) months where necessary, taking into account the complexity and number of requests. You will be informed of any extension within the initial one-month period.

Identity Verification. To prevent unauthorised disclosure, Pladinum may require you to verify your identity before processing a request. We will request the minimum information necessary for verification and will not retain identity documents beyond the duration required to process the request.

10. Security Measures

10.1 Pladinum implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 GDPR. These measures include:

Encryption: All data in transit is protected by TLS/SSL encryption. Sensitive data at rest is encrypted using industry-standard algorithms.

Access Controls: Access to personal data is restricted to authorised personnel on a need-to-know basis, enforced through role-based access controls, strong password policies, and multi-factor authentication.

Infrastructure Security: Firewalls, intrusion detection and prevention systems (IDS/IPS), DDoS mitigation, antivirus software, and continuous monitoring protect the network and server infrastructure.

Physical Security: Data centre facilities operated by our infrastructure partners (Leaseweb) maintain physical access controls, environmental protections, and 24/7 surveillance.

Employee Training: All employees with access to personal data receive regular training on data protection obligations, confidentiality, and security best practices.

Incident Response: Pladinum maintains a documented incident response plan for identifying, containing, and remediating security incidents.

10.2 Pladinum's security framework is designed to align with industry-standard practices. Security measures are regularly reviewed and updated to address evolving threats.

11. Data Breach Notification

11.1 In the event of a personal data breach, Pladinum shall notify the competent supervisory authority (AEPD) without undue delay and, where feasible, within seventy-two (72) hours of becoming aware of the breach, in accordance with Article 33 GDPR, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.

11.2 Where the breach is likely to result in a high risk to the rights and freedoms of affected individuals, Pladinum shall also notify the affected data subjects without undue delay, in accordance with Article 34 GDPR, providing clear information about the nature of the breach, the likely consequences, and the measures taken or proposed to address it.

11.3 Where Pladinum acts as a data processor, it shall notify the data controller (Customer) of a personal data breach without undue delay after becoming aware of it, enabling the controller to fulfil its own notification obligations.

12. Cookies and Tracking Technologies

Pladinum uses cookies and similar tracking technologies on its Site to ensure functionality, analyse usage, and manage consent preferences. Detailed information about the cookies we use, their purposes, durations, and your options for managing them is provided in our Cookie Policy, available on the Site.

Cookie consent is managed through CookieFirst (Digital Data Solutions BV, Netherlands). You can adjust your preferences at any time via the cookie settings accessible in the Site footer.

13. Children's Data

Pladinum's Services are not directed at individuals under the age of eighteen (18). Pladinum does not knowingly collect personal data from children. If we become aware that we have collected personal data from a child without appropriate parental or guardian consent, we will take steps to delete such data without undue delay.

If you believe that a child has provided personal data to Pladinum, please contact us at privacy@pladinum.com so that we can take appropriate action.

14. Automated Decision-Making and Profiling

14.1 Pladinum does not currently engage in solely automated decision-making (including profiling) that produces legal effects or similarly significantly affects data subjects, as described in Article 22 GDPR.

14.2 Pladinum may use automated tools for fraud detection, abuse prevention, and security monitoring. These tools may flag activities for review but do not, by themselves, make final decisions affecting your rights or Services without human oversight.

14.3 Should Pladinum introduce automated decision-making in the future, this policy will be updated and affected individuals will be informed, with appropriate safeguards including the right to obtain human intervention, to express their point of view, and to contest the decision.

15. Direct Marketing

15.1 Pladinum may send you marketing communications about products, services, or promotions that we believe may be of interest to you, but only where you have provided your prior opt-in consent.

15.2 Opt-Out. You may withdraw your consent to receive marketing communications at any time by: (i) clicking the “unsubscribe” link included in each marketing email; (ii) contacting privacy@pladinum.com; or (iii) adjusting your preferences in the customer portal.

15.3 Withdrawal of consent to marketing communications does not affect service-related communications (such as billing notifications, security alerts, or service updates), which are sent on the basis of contractual necessity.

16. Third-Party Websites and Links

The Site may contain links to websites operated by third parties (including social media platforms, partner websites, and event pages). Pladinum is not responsible for the content, privacy practices, or security of third-party websites. We encourage you to review the privacy policy of any third-party site before providing personal data.

17. Confidentiality of Communications

The existence and content of communications transmitted via Pladinum’s network (including email traffic, hosted data, and other electronic communications) are protected by the principle of telecommunications secrecy. Pladinum and its employees shall not access the content of such communications except where: (i) required by law or court order; (ii) necessary to protect the integrity and security of the network; or (iii) expressly authorised by the Customer.

18. Website and Portal

18.1 Pladinum’s website is provided for informational and service purposes. All content is offered on an “as-is” basis. Pladinum reserves the right to modify, restrict, or revoke access to any part of the website at any time.

18.2 Access to restricted areas (such as the customer portal) requires the provision of personal data, which is processed in accordance with this Privacy Policy.

19. Changes to This Privacy Policy

19.1 Pladinum reserves the right to update this Privacy Policy at any time to reflect changes in our data processing practices, legal requirements, or business operations.

19.2 Material changes will be communicated through a prominent notice on the Site and, where appropriate, by direct notification (e.g., email). The “Last revised” date at the top of this document indicates when the most recent revision was made.

19.3 We encourage you to review this policy periodically.

20. Contact Information and Complaints

For any questions, requests, or complaints regarding this Privacy Policy or the processing of your personal data, please contact us:

Pladinum Group SL

Attn: Data Protection

Avenida de Manolete 3a

29660 Marbella, Malaga (ES)

Email: privacy@pladinum.com

Telephone: +34 697 9898 40

If you are not satisfied with our response, you have the right to lodge a complaint with the competent supervisory authority:

Agencia Española de Protección de Datos (AEPD)

C/ Jorge Juan, 6
28001 Madrid, Spain
www.aepd.es