Privacy Policy of Provice Informatika Kft. (For Information Only)

Last updated: October 6, 2025

Note: The only legally binding version is the Hungarian "Adatkezelési Tájékoztató." This English text is provided solely for your reference.

1. INTRODUCTION

Provice Informatika Kft. ("Provice," "we," "us," "our") organizes professional events and activities (each, an "Event"). This Policy explains how we lawfully collect and process personal data of Event participants ("you," "your") under:

• Act CXII of 2011 on Informational Self-Determination and Freedom of Information (Infotv.)
• EU Regulation 2016/679 (GDPR)

We implement all reasonable technical and organizational measures to safeguard your data. By registering for or attending any Event, you consent to the data practices described herein, including AI-driven processing and stricter cookie requirements effective 2025.

2. DATA CONTROLLER DETAILS

Provice Informatika Korlátolt Felelősségű Társaság
Registered seat: 1037 Budapest, Montevideo u. 9., 1st floor
Company registration no.: 01-09-906168
Tax no.: 14490411-2-41
Email: provice@provice.hu
Phone: +36-20-435-5142

3. WEBSITE VISITS

When you visit www.dynatrace.provice.eu, we automatically collect:

Purpose: site operation, analytics, UX improvements, security incident handling
Legal basis: our legitimate interest (GDPR 6(1)(f))
Data: IP address; browser type and version; OS; pages visited; visit time and duration; referrer URL
Cookies: essential cookies load automatically; analytics/marketing cookies load only after explicit consent per 2025 rules

Retention: up to 6 months after your visit
Access: system administrators, web developers, and an anonymous Google Analytics processor

IMPORTANT: From 2025, all non-essential cookies are blocked until you grant explicit consent. You may withdraw cookie consent at any time.

4. LEGAL BASIS & PURPOSES

Purpose	Legal Basis	Details
Event registration & participation	GDPR 6(1)(b) – contract performance	Managing registration, running the Event, communications
Invoicing & accounting	GDPR 6(1)(c) – legal obligation	Compliance with accounting and VAT laws
Marketing communications	GDPR 6(1)(f) – legitimate interest or GDPR 6(1)(a) – consent	Professional follow-up, similar Event invitations
Photo/video recording	GDPR 6(1)(a) – explicit consent	Event documentation, promotional use
AI-based profiling	GDPR 6(1)(a) – explicit consent	Personalized recommendations (DPIA mandatory)
Automated decision-making	GDPR 22 – explicit consent	AI decisions (you may request human review)
Backups & archiving	GDPR 6(1)(f) – legitimate interest	Data security, business continuity

NEW for 2025: Every AI-based processing requires a dedicated Data Protection Impact Assessment, and you may request human intervention in any automated decision.

5. CATEGORIES OF PERSONAL DATA

5.1 Registration & Contact Data

- Full name
- Email address
- Phone number
- Employer name
- Job title
- Billing address (if applicable)

5.2 Event-Generated Data

- Attendance details (presence, duration)
- Photographs and audio/video recordings (with explicit consent)
- Areas of interest, feedback
- Network connection logs

5.3 Technical Data

- IP address and other network identifiers
- Cookie identifiers
- Device details (browser, OS)
- Website usage statistics

DATA MINIMIZATION: We process only the minimum data necessary for each purpose.

6. RETENTION PERIODS

Data Category	Retention	Deletion Method
Event registration data	2 years after Event	Automatic deletion
Website logs	Up to 6 months	Automatic deletion
Invoicing data	8 years (accounting law)	Deleted after legal term
Marketing data	Until consent withdrawal, max 3 years	On request or automatically
Photos and recordings	Until consent withdrawal	Deleted on request
AI profiling data	Until consent withdrawal	Deleted on request

Deletion Rules:

- Secure, irreversible deletion
- Removal from backup archives
- AI profiles deleted immediately on request
- You may request immediate deletion of any data, except those we must retain by law

7. DATA PROCESSORS

Processor	Service	Data Processed	Location
Microsoft Corporation	Microsoft 365	All data categories	EU region
Wix.com Inc.	Website analytics (anonymous)	Visit stats, contact data	USA (100 Gansevoort St, New York, NY)
Zoho Corporation B.V.	Customer relationship management	Contact data	Utrecht, Netherlands

Processor Guarantees:

- Written contracts in place
- GDPR compliance obligations
- Process only per our instructions
- International transfers only under adequacy decisions or sufficient safeguards
- Regular audits and compliance checks

8. TECHNICAL & ORGANIZATIONAL MEASURES

8.1 Access Control

- Role-based access
- Two-factor authentication on critical systems
- Regular rights review
- Access logging and monitoring

8.2 Encryption

- TLS 1.3 in transit
- AES-256 at rest
- Dedicated key management
- End-to-end encryption for sensitive data

8.3 Security Monitoring

- 24/7 security monitoring
- Automated threat detection
- Incident response process
- Regular penetration tests and vulnerability scans

8.4 Organizational Safeguards

- DPO appointment (if required)
- Ongoing privacy training
- Confidentiality agreements
- Mandatory DPIAs
- Incident reporting within 72 hours

NIS2 Compliance: These measures meet Hungary's 2025 NIS2 requirements.

9. YOUR RIGHTS

Under the GDPR, you may:

- Be informed about how we use your data (Arts. 13–14)
- Access your data (Art. 15)
- Rectify inaccurate data (Art. 16)
- Erase data ("right to be forgotten," Art. 17)
- Restrict processing (Art. 18)
- Data portability (Art. 20)
- Object to processing (Art. 21)
- Challenge automated decisions and profiling (Art. 22)
- Withdraw consent at any time (cookies/profiling)

10. REQUEST HANDLING

10.1 Submission Methods

• Email: marketing@provice.hu
• Postal: 1037 Budapest, Montevideo u. 9., 1st floor
• In person: by prior appointment at our registered office
• Phone: +36-20-435-5142 (info only; requests must be in writing)

10.2 Procedure

• Receipt and registration of request
• Identity verification (ID copy required)
• Evaluation and response preparation
• Response sent within 30 days (extended by 60 days for complex cases)

10.3 Fees

First request free. Unfounded or excessive repeat requests may incur a reasonable fee.

11. COMPLAINTS

If you believe we breached your GDPR rights, you may complain to:

Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)
1055 Budapest, Falk Miksa utca 9–11.
Mailing: 1363 Budapest, Pf. 9
Email: ugyfelszolgalat@naih.hu
Tel: +36 1 391 1400

You may also pursue judicial remedies without affecting other administrative options.

12. DATA BREACH HANDLING

In case of a personal data breach, we will:

• Immediately investigate and contain the breach
• Notify NAIH within 72 hours if likely to risk data subjects' rights
• Inform affected individuals without undue delay if high risk is confirmed
• Record the incident and corrective actions
• Implement preventive measures

13. LEGAL REFERENCES

• GDPR (EU) 2016/679
• Infotv. (Act CXII/2011)

- Civil Code (Act V/2013)
- Accounting Act (Act C/2000)
- National Security Services Act (Act LXXVII/2017)
- Digital State Amendments Act (Act XXXII/2025)
- Proposed ePrivacy Regulation (cookie rules)

14. FINAL PROVISIONS

14.1 Effective Date & Amendments

This Policy takes effect October 6, 2025, replacing the November 25, 2024 version. We may amend it; material updates will be emailed to you and posted online.

14.2 2025 Summary of Key Changes

- Pre-consent cookie blocking
- New AI profiling and automated decision rules
- Mandatory DPIAs for AI projects
- Enhanced NIS2 security measures
- Planned online request portal
- Shorter response time (standard 30 days, 25 days in most cases)

14.3 Language of Authority

The Hungarian version is authoritative. Translations are for your convenience only.

Budapest, October 6, 2025