DATA PROCESSING AGREEMENT

DPA

ITPACK SHIELD – www.itpackshield.com

Effective date: 26 September 2026
Last updated: 26 September 2026

1. Purpose and scope of the Agreement

This Data Processing Agreement (the “DPA” or “Agreement”) sets out the terms under which Heftner Group Kft. processes personal data on behalf of the Customer in the course of providing the ITPACK SHIELD service.

This DPA forms part of the service agreement, accepted offer, order or other individual agreement relating to the ITPACK SHIELD service (the “Main Agreement”) where the Main Agreement provides for the application of, or refers to, this DPA.

This DPA applies to processing operations in respect of which the Customer using the ITPACK SHIELD service is the controller within the meaning of Regulation (EU) 2016/679 of the European Parliament and of the Council (“GDPR”), and Heftner Group Kft. acts as processor on behalf of the Customer.

This DPA does not apply to processing activities in which Heftner Group Kft. acts as an independent controller, including in particular its own customer relationship, contractual, invoicing, legal or statutory processing activities. Such processing is governed by the applicable Privacy Notice of Heftner Group Kft.

2. The parties

2.1. Controller

The Customer identified in the Main Agreement and using the ITPACK SHIELD service (hereinafter: the “Customer” or “Controller”).

2.2. Processor

Heftner Group Kft.
Registered office: 2013 Pomáz, Vróci utca 12., Hungary
Company registration number: 13-09-123295
Tax number: HU12710658
E-mail: sales@it-pack.com
Technical support: support@it-pack.com
Website: www.itpackshield.com
(hereinafter: the “Processor”).

3. Subject matter of processing

The ITPACK SHIELD cybersecurity platform receives, organises and analyses security events and log data originating from the Customer’s IT environment. The scope of data sources depends on the Customer’s infrastructure, the systems connected to the platform and the individual service configuration.

Some log and security event data may constitute personal data where they relate directly or indirectly to an identified or identifiable natural person.

4. Purpose of processing

The sole purpose of the processing is to provide the ITPACK SHIELD cybersecurity service and perform the Main Agreement. In this context, processing may in particular serve the following purposes:

- receiving and processing security events;
- analysing log data;
- identifying and correlating relationships between different security events;
- supporting the detection of anomalous or potentially dangerous activities;
- assessing and interpreting security events and attack patterns;

- cybersecurity decision support;
- displaying security events and risks;
- supporting the Customer's IT security activities;
- in the case of Shield Care+, expert monitoring, event analysis and incident assessment;
- troubleshooting, testing, backup and recovery necessary for operating the service.

The Processor may not use the Customer's personal data for its own purposes other than the service purposes defined in the Main Agreement and this DPA, unless required to do so by applicable Union or Member State law.

5. Nature and location of processing

The primary processing of ITPACK SHIELD data takes place within the Customer's local IT environment, in the dedicated ITPACK SHIELD service environment. Processing may include receiving, collecting, organising, structuring, storing, retrieving, comparing, correlating, analysing, security assessment, displaying and deleting data.

For Shield Care+, processing may also include review and assessment of security events by duly authorised experts of Heftner Group Kft.

Data required for operating the service, backup, troubleshooting or testing may be transferred to an IT environment under the Processor's own control only to the extent and for the period necessary. Such processing does not constitute transfer of the data to an external sub-processor or public AI service provider.

6. Duration of processing and retention period

As a general rule, processing continues for the duration of the Main Agreement relating to the ITPACK SHIELD service.

The default active retention period for log and security event data is 30 days. The Controller's documented instruction, the individual service configuration or the Main Agreement may provide for a different period, provided that the different period is lawful and technically feasible.

After expiry of the default retention period, the relevant data may be deleted, overwritten or anonymised as part of the normal operation of the system. Backups and data remaining after termination of the Main Agreement are governed by Section 19 of this DPA.

7. Types of personal data processed

Depending on the Customer's IT environment and the connected data sources, log and security event data processed by ITPACK SHIELD may in particular contain the following categories of personal data:

Data category	**Possible examples**
Network identifiers	IP addresses, source and destination addresses
User identifiers	username, account identifier, technical identifier
Authentication events	successful and failed logins, access events
Device data	device name, device identifier, system and client information
Network events	connections, ports, protocols and technical data related to communications
Security events	alerts, attack patterns, detected anomalies
Log data	personal data contained in logs originating from connected systems

Other technical data	technical information originating from connected systems that can be linked to a natural person

ITPACK SHIELD does not require the Customer to provide separate personal data for AI analysis. AI analysis is performed on security events and log data that are otherwise processed by the platform.

8. Categories of data subjects

Depending on the Customer's IT environment, data subjects may in particular include the following natural persons:

- the Customer's employees;
- users of the Customer's systems;
- the Customer's contractors and contributors;
- users of the Customer's business partners;
- the Customer's customers, where their data appear in the relevant systems;
- other persons interacting with the Customer's IT systems;
- persons attempting unauthorised access, where the event data can be linked to a natural person.

9. Local AI-assisted analysis

ITPACK SHIELD uses locally operated, AI-assisted analysis to support the interpretation of security events and log data. AI analysis takes place within the ITPACK SHIELD service environment.

For the purpose of AI analysis, the Customer's log data, security events, prompts and analytical data derived from them are not transmitted to an external public AI service provider. The AI function forms part of ITPACK SHIELD's internal processing workflow.

The purpose of AI-assisted analysis includes supporting event interpretation and correlation, assessing potential risks, producing human-readable summaries, and generating proposed security measures and decision-support information.

Analysis, summaries or recommendations generated by AI constitute decision-support information. This ITPACK SHIELD function does not, by itself, make an automated decision concerning a natural person that produces legal effects or similarly significantly affects that person.

10. Documented instructions of the Controller

The Processor shall process personal data only on documented instructions from the Controller, including with regard to transfers of personal data to a third country or an international organisation, unless Union or Member State law applicable to the Processor requires other processing. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

Documented instructions may include, in particular, the Main Agreement, this DPA, the accepted service configuration, the data sources and integrations specified by the Customer, and the Customer's documented support or technical requests.

If, in the Processor's opinion, an instruction infringes the GDPR or other applicable Union or Member State data protection provisions, the Processor shall immediately inform the Controller.

11. Obligations of the Controller

The Controller is responsible for the lawfulness of the original collection and processing of personal data transmitted to the ITPACK SHIELD system. Its responsibilities include in particular:

- determining the appropriate legal basis for processing;

- providing appropriate information to data subjects;
- complying with the principles of data minimisation and purpose limitation;
- determining which systems and data sources are connected to the ITPACK SHIELD service;
- ensuring that the processing of data transmitted to the Processor is lawful;
- where necessary, establishing appropriate internal authorisations, policies and data protection measures.

The Processor does not determine the original purpose or legal basis for the collection of the Customer's log data.

12. Confidentiality

The Processor shall ensure that access to the Customer's personal data is limited to authorised persons for whom such access is necessary to provide the service. Persons authorised to process personal data shall be subject to an appropriate obligation of confidentiality, which shall continue after termination of the Main Agreement.

The Processor shall also treat as confidential any security and technical information learned about the Customer's systems, network, security events, configuration, vulnerabilities and IT infrastructure.

13. Data security

The Processor shall implement technical and organisational measures in accordance with Article 32 GDPR, appropriate to the nature, scope, context and purposes of processing and to the risk to the rights and freedoms of natural persons. Such measures are intended in particular to support:

- protection of the confidentiality, integrity and availability of personal data;
- prevention of unauthorised access and restriction of access rights;
- protection of IT systems and communications;
- detection and handling of security events;
- use of backup and recovery processes where necessary;
- regular review of the effectiveness of technical and organisational measures in a manner proportionate to the risks.

The detailed configuration of technical and organisational measures may constitute security-sensitive information. The Processor is not required to disclose publicly details that could reduce the security of ITPACK SHIELD or the Customer's systems; this does not affect the Controller's audit rights under Article 28 GDPR.

14. Remote access and provider access

For implementation, configuration, maintenance, troubleshooting or technical support of ITPACK SHIELD, the Customer may, where necessary, provide the Processor with access through a secure VPN connection or another appropriately protected technical solution. For Shield Care+, such access may also be used to provide the agreed expert monitoring and event assessment.

The Processor shall use such access solely for authorised service tasks, only to the extent necessary and with privileges restricted to the minimum required.

15. Sub-processors

As at the effective date of this DPA, the Processor does not use any sub-processor for personal data processing activities carried out on behalf of the Controller within the ITPACK SHIELD service.

The primary processing of ITPACK SHIELD data takes place in the Customer's local IT environment, and customer data are not transferred to an external public AI service provider or other third party for AI-assisted analysis.

If the Processor intends to engage a sub-processor in the future, it may do so on the basis of the Controller's general written authorisation. The Processor shall provide appropriate prior information regarding the intended engagement

or replacement of a sub-processor and shall give the Controller a reasonable opportunity to raise a substantiated objection on data protection grounds.

The Processor shall impose on the sub-processor, by written agreement, data protection obligations at least equivalent to those set out in this DPA and required by Article 28(4) GDPR. The Processor shall remain responsible to the Controller under the GDPR for the performance of the sub-processor's obligations.

16. Assistance with data subject rights

Where a data subject contacts the Processor directly regarding personal data processed within ITPACK SHIELD, the Processor shall, unless otherwise required by law, forward the request to the Controller and shall not independently determine the merits of the request.

Taking into account the nature of the processing, the Processor shall assist the Controller, by appropriate technical and organisational measures and to the extent reasonably possible, in fulfilling data subject rights under Chapter III GDPR.

17. Personal data breach

If the Processor becomes aware of a personal data breach affecting personal data processed on behalf of the Customer, it shall notify the Controller without undue delay.

Based on the information available to it, the Processor shall provide information on the nature of the breach, the categories and, where possible, approximate number of affected data subjects and personal data records, the likely consequences, and the measures taken or proposed. Where all information is not available at the same time, it may be provided in phases without undue further delay.

It is the Controller's responsibility to determine whether the breach gives rise to a notification or communication obligation towards the supervisory authority or data subjects, unless applicable law imposes an obligation directly on the Processor.

18. Assistance with other GDPR obligations of the Controller

Taking into account the nature of processing and the information available to it, the Processor shall provide reasonable assistance to the Controller in ensuring compliance with the obligations under Articles 32–36 GDPR. Where necessary, this may include assistance with assessing data security, handling personal data breaches, supporting data protection impact assessments, and providing information available to the Processor that is required for prior consultation with the supervisory authority.

19. Deletion or return of data

Following termination of the Main Agreement, the Processor shall, at the choice of the Controller, delete or – where technically reasonably feasible in the relevant system – return the personal data processed on behalf of the Controller and delete existing copies, unless Union or Member State law requires further storage of the data.

The Controller shall notify the Processor by the date of termination if it requests return of the data. If the Controller does not request return, the Processor may delete the data in accordance with the ordinary deletion process following termination of the service.

Data remaining in regular backups may be deleted in accordance with the normal backup retention and overwrite cycle, provided that no further active processing of such data takes place during that period unless required for recovery, security or legal reasons. Access to backups shall remain restricted to the minimum necessary during this period.

20. Special categories of personal data and unnecessary content

ITPACK SHIELD is not specifically intended for processing special categories of personal data under Article 9 GDPR or personal data relating to criminal convictions and offences under Article 10 GDPR. The Customer shall reasonably avoid transmitting to ITPACK SHIELD data that are not necessary for providing the cybersecurity service.

Where, due to the characteristics of the Customer's IT environment, the occurrence of such data is unavoidable or reasonably foreseeable, the Controller is responsible for ensuring an appropriate legal basis and safeguards, and the parties may agree additional data protection or security measures where necessary.

21. International data transfers

The Processor may transfer personal data processed on behalf of the Customer within ITPACK SHIELD outside the European Economic Area only on the Controller's documented instructions and subject to the conditions set out in Chapter V GDPR, unless Union or Member State law requires such transfer.

The current service architecture does not require customer data to be transferred to an external AI service provider. AI-assisted analysis is performed locally within the ITPACK SHIELD service environment. Backup, testing or troubleshooting operations performed under the Processor's own control do not in themselves constitute a transfer to a third party.

22. Audit and demonstration of compliance

The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with its obligations under Article 28 GDPR and this DPA and shall allow for and contribute to lawful and proportionate audits conducted by the Controller or an independent auditor mandated by the Controller.

Except in the case of an urgent personal data breach or a binding requirement of a competent authority, audits shall be conducted at a mutually agreed time and without unreasonably disrupting the operation of the service. Audits shall protect other customers' data, the security of ITPACK SHIELD and the Processor's systems, business secrets and intellectual property.

Where compliance can reasonably be demonstrated by documents, certifications, audit reports or other appropriate evidence, the parties shall use such means as the primary method. Documented additional costs of an audit requested by the Controller that materially exceeds customary compliance information may, where not prohibited by law, be borne by the Controller, unless the audit identifies a material breach of contract or law by the Processor.

23. Records and cooperation with supervisory authorities

Where and to the extent required by Article 30(2) GDPR, the Processor shall maintain a record of categories of processing activities carried out on behalf of the Controller and shall cooperate with the competent supervisory authority to the extent required by the GDPR.

24. Precedence of the DPA and liability

If there is any conflict between this DPA and the data protection provisions of the Main Agreement, this DPA shall prevail with respect to the processing of personal data, unless the parties expressly agree stricter or more specific terms for the relevant processing.

The parties' data protection liability shall be governed by the GDPR, applicable data protection law, the Main Agreement and, where lawfully applicable, its limitations of liability. Nothing in this DPA shall be construed as excluding or limiting liability that cannot be excluded or limited under the GDPR.

25. Amendment of the DPA

The Processor may amend this DPA in particular due to changes in law, changes in the manner in which the service processes data, security or technological changes, or the engagement of a new sub-processor. Any amendment shall not reduce the mandatory data protection safeguards required by Article 28 GDPR.

The Processor shall provide appropriate prior information regarding material amendments affecting existing customers. Where an amendment concerns the engagement of a new sub-processor, the procedure set out in Section 15 shall apply.

26. Governing law and language

This DPA is governed by the GDPR and, unless mandatory law or the individual Main Agreement provides otherwise, the laws of Hungary.

The DPA may be published in Hungarian and English. Unless otherwise agreed and to the extent permitted by applicable law, in the event of any discrepancy in interpretation, the Hungarian-language version shall prevail.

ANNEX 1

Summary of processing

Item	Definition
Controller	The Customer using the ITPACK SHIELD service
Processor	Heftner Group Kft.
Subject matter of processing	Processing necessary for providing the ITPACK SHIELD cybersecurity service
Purpose	security monitoring, event and log analysis, correlation, risk assessment, decision support and, for Shield Care+, expert monitoring and incident assessment
Duration	the duration of the service relationship and the necessary deletion or return period thereafter
Types of data	network identifiers, IP addresses, user identifiers, authentication events, device data, security events and log data
Data subjects	the Customer’s employees, users, partners, customers and other natural persons interacting with the Customer’s systems
AI analysis	locally within the ITPACK SHIELD service environment; customer data are not transferred to an external AI service provider for AI analysis
Special categories	their processing is not a purpose of the service; where they occur, Section 20 applies
Retention period	30 days by default; may differ based on a documented individual instruction or configuration
Deletion/return	in accordance with Section 19 of this DPA and the individual Main Agreement
Sub-processors	currently no sub-processors

ANNEX 2

Technical and organisational measures

The Processor applies technical and organisational measures appropriate to the nature and risk of the processing. Depending on the relevant technical environment, these may in particular cover:

- access control and authorisation management;
- appropriate authentication mechanisms;
- network security measures;
- secure remote access;
- system and security logging;
- management of system and component updates;
- vulnerability management;
- backup and recovery;
- incident detection and incident management processes;
- secure communications;
- restriction of access rights to the minimum necessary;
- confidentiality obligations;
- support for recoverability and business continuity appropriate to the nature of the service;
- regular review and, where necessary, modification of security measures.

This public DPA intentionally does not include detailed network, system, access or protection configurations whose disclosure could endanger the cybersecurity of ITPACK SHIELD or its customers.

ANNEX 3

Current sub-processor status

As at the effective date of this DPA, Heftner Group Kft. does not use any sub-processor for processing customer data within the ITPACK SHIELD service.

The primary processing and AI-assisted analysis of ITPACK SHIELD data are performed locally. Customer data are not transferred to an external public AI service provider for AI analysis. Backup, testing or troubleshooting operations necessary for the operation of the service and performed under the own control of Heftner Group Kft. do not constitute the engagement of an external sub-processor.