DATA PROCESSING AGREEMENT

Auftragsverarbeitungsvertrag (AVV)

between

INTECH Automation & Intelligence GmbH

empowergpt.ai · Data Processor

and

[CLIENT COMPANY NAME]

[Client Address] · Data Controller

Document Version	Effective Date	Regulatory Basis
v2.2 (2026)	[_____]	GDPR (EU) 2016/679

CONFIDENTIAL — NOT FOR DISTRIBUTION

Preamble

This Data Processing Agreement ("DPA" or "Agreement") is entered into between INTECH Automation & Intelligence GmbH ("Processor" or "INTECH Automation & Intelligence") and the entity identified as Data Controller in Annex I ("Controller" or "Client"), each a "Party" and together the "Parties".

This DPA forms an integral part of the Master Services Agreement ("MSA") or subscription agreement between the Parties governing the Controller's use of the INTECH Automation & Intelligence platform and associated services ("Services"). In the event of any conflict between this DPA and the MSA regarding data protection matters, this DPA shall prevail.

This DPA is designed to comply with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the "GDPR"), including any applicable national implementing legislation and successor regulations. The structure and obligations herein reflect best practices adopted across the enterprise AI sector and align with guidance from the European Data Protection Board ("EDPB").

The Parties acknowledge that INTECH Automation & Intelligence operates as an AI-powered enterprise platform that may process personal data submitted by Controller or its authorised users during normal use of the Services. The purpose and nature of processing is described in Annex I.

---

1. Definitions and Interpretation

1.1 In this DPA, the following terms have the meanings set out below. Capitalised terms not defined herein shall have the meanings ascribed to them in the GDPR or the MSA.

Term	Definition
"Applicable Data Protection Law"	The GDPR, together with any applicable national data protection laws in EU/EEA Member States, the UK GDPR, Swiss Federal Act on Data Protection (nFADP) where applicable, and any successor or supplementary legislation.
"Controller"	The natural or legal person that determines the purposes and means of the processing of Personal Data (GDPR Art. 4(7)).
"Data Subject"	An identified or identifiable natural person whose Personal Data is processed under this DPA (GDPR Art. 4(1)).
"EEA"	The European Economic Area, comprising EU Member States plus Iceland, Liechtenstein, and Norway.
"Personal Data"	Any information relating to an identified or identifiable natural person as defined in GDPR Art. 4(1).
"Personal Data Breach"	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data (GDPR Art. 4(12)).
"Processor"	A natural or legal person that processes Personal Data on behalf of the Controller (GDPR Art. 4(8)).
"Processing"	Any operation performed on Personal Data, including collection, storage, use, disclosure, or erasure (GDPR Art. 4(2)).
"Restricted Transfer"	A transfer of Personal Data to a third country not recognised as providing an adequate level of protection under GDPR Chapter V.

"SCCs"	Standard Contractual Clauses adopted by the European Commission pursuant to GDPR Art. 46(2).
"Services"	The INTECH Automation & Intelligence enterprise AI platform and all related services as described in the MSA.
"Special Category Data"	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life or sexual orientation (GDPR Art. 9(1)).
"Sub-processor"	Any third-party processor engaged by INTECH Automation & Intelligence to carry out processing activities on behalf of the Controller (GDPR Art. 28(4)).
"TOMs"	Technical and Organisational Measures implemented to ensure the security of Personal Data (GDPR Art. 32).

2. Scope and Role of the Parties

2.1 Roles. The Controller determines the purposes and means of processing Personal Data submitted to the Services. INTECH Automation & Intelligence acts as Processor in respect of Personal Data processed through the Services on the Controller's behalf, in accordance with GDPR Art. 28.

2.2 Instructions. INTECH Automation & Intelligence shall process Personal Data only on documented instructions from the Controller, which include: (a) this DPA; (b) the MSA; (c) the Service configuration and settings; and (d) any additional written instructions agreed by the Parties. Processing for any other purpose requires prior written consent.

2.3 Incompatible Instructions. If INTECH Automation & Intelligence considers that an instruction infringes Applicable Data Protection Law, it shall promptly inform the Controller without delay. INTECH Automation & Intelligence shall not be required to follow instructions that would put it in breach of law.

2.4 Controller Obligations. The Controller warrants and represents that: (a) it has a valid legal basis for any processing of Personal Data it instructs INTECH Automation & Intelligence to perform; (b) it has provided all required notices to Data Subjects; (c) it will not upload Special Category Data unless a separate written addendum is executed; and (d) it will use the Services in compliance with Applicable Data Protection Law.

2.5 Scope of this DPA. This DPA applies to all processing of Personal Data by INTECH Automation & Intelligence as Processor on behalf of the Controller in connection with the Services. It does not apply to processing for which INTECH Automation & Intelligence acts as an independent Controller (e.g., account management, billing, legal compliance).

---

3. Processor Obligations

3.1 General Obligations

INTECH Automation & Intelligence shall, in relation to Personal Data processed on behalf of the Controller:

- process Personal Data only on documented instructions of the Controller, unless processing is required by EU or Member State law to which INTECH Automation & Intelligence is subject (Art. 28(3)(a));
- ensure that persons authorised to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b));
- implement and maintain appropriate technical and organisational measures as set out in Section 5 and Annex II of this DPA (Art. 28(3)(c), Art. 32);
- respect the conditions for engaging Sub-processors as set out in Section 7 of this DPA (Art. 28(3)(d));

- taking into account the nature of processing, assist the Controller by appropriate technical and organisational measures in fulfilling the Controller's obligation to respond to requests for exercising Data Subjects' rights (Art. 28(3)(e));
- assist the Controller in ensuring compliance with its obligations under Arts. 32–36 GDPR (security, breach notification, DPIAs, prior consultation) (Art. 28(3)(f));
- at the Controller's choice, delete or return all Personal Data upon termination of the Services and delete existing copies unless EU or Member State law requires storage (Art. 28(3)(g));
- make available to the Controller all information necessary to demonstrate compliance with Art. 28 GDPR and allow for and contribute to audits and inspections (Art. 28(3)(h)).

4. Data Subject Rights

4.1 Facilitation of Rights. INTECH Automation & Intelligence shall, taking into account the nature of the processing, assist the Controller in fulfilling its obligations to respond to requests by Data Subjects to exercise their rights under Chapter III GDPR, including rights of: access (Art. 15); rectification (Art. 16); erasure / right to be forgotten (Art. 17); restriction of processing (Art. 18); data portability (Art. 20); objection (Art. 21); and rights related to automated decision-making (Art. 22).

4.2 Timelines. Upon receiving a request from a Data Subject directly, INTECH Automation & Intelligence shall: (a) without undue delay and in any event within three (3) business days, forward the request to the Controller; and (b) not respond directly to the Data Subject unless authorised in writing by the Controller or required by applicable law.

4.3 Technical Measures. INTECH Automation & Intelligence shall maintain technical capabilities enabling the Controller to: (a) export Personal Data in a structured, commonly used, machine-readable format (Art. 20); (b) delete or anonymise specific user data records on request; (c) restrict processing for specific users or categories; and (d) provide Data Subjects with a copy of their data.

4.4 Costs. INTECH Automation & Intelligence's assistance with Data Subject rights requests is included within the Services fee. Where requests are manifestly unfounded or excessive, INTECH Automation & Intelligence may charge reasonable costs for extraordinary effort, subject to prior written notice and agreement.

4.5 No Independent Decision-Making. INTECH Automation & Intelligence shall not make any decisions on behalf of the Controller regarding whether a Data Subject's rights should be granted or denied. Any such decision is solely the Controller's responsibility.

---

5. Security of Processing

5.1 General Security Obligation. INTECH Automation & Intelligence shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, costs of implementation, and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons (Art. 32(1) GDPR).

5.2 Specific Measures. Without prejudice to the generality of clause 5.1, INTECH Automation & Intelligence shall implement the measures described in Annex II to this DPA, which shall include as a minimum:

- pseudonymisation and encryption of Personal Data (Art. 32(1)(a));
- the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services (Art. 32(1)(b));
- the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident (Art. 32(1)(c));

- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing (Art. 32(1)(d)).

5.3 Security Reviews. INTECH Automation & Intelligence shall regularly review and update its security measures to reflect changes in risk, technology, and best practice. INTECH Automation & Intelligence shall maintain relevant security certifications (including ISO 27001 and SOC 2 Type II) and shall provide copies of certificates or relevant audit reports to the Controller upon request.

5.4 Tenant Isolation. INTECH Automation & Intelligence shall ensure strict logical separation between the Controller's data and data of other customers. The Controller's Personal Data shall not be accessible by any other customer of INTECH Automation & Intelligence.

5.5 AI-Specific Security. In the context of AI processing: (a) the Controller's data shall not be used to train foundational AI models without explicit written consent; (b) model outputs containing Personal Data shall be subject to output filtering controls; (c) prompt injection and adversarial input controls shall be maintained; and (d) model access to Personal Data shall be limited to what is strictly necessary for service delivery.

6. Personal Data Breach Notification

6.1 Detection and Assessment. INTECH Automation & Intelligence shall maintain procedures to detect, assess, and respond to Personal Data Breaches. INTECH Automation & Intelligence shall maintain incident response capabilities as further described in Annex II.

6.2 Notification to Controller. Without undue delay, and where feasible within 36 hours of becoming aware of a confirmed Personal Data Breach, INTECH Automation & Intelligence shall notify the Controller. Notification shall include, to the extent then known:

- a description of the nature of the Personal Data Breach including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
- the name and contact details of the data protection officer or other contact point from whom more information can be obtained;
- a description of the likely consequences of the Personal Data Breach;
- a description of the measures taken or proposed to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

6.4 Cooperation. INTECH Automation & Intelligence shall cooperate fully with the Controller in the Controller's compliance with its notification obligations to supervisory authorities (Art. 33 GDPR) and to Data Subjects (Art. 34 GDPR). INTECH Automation & Intelligence shall not communicate the Personal Data Breach to Data Subjects or supervisory authorities without the Controller's prior written consent, unless required to do so by applicable law.

7. Sub-processors

7.1 General Authorisation. The Controller hereby grants INTECH Automation & Intelligence general written authorisation to engage Sub-processors, subject to the conditions in this Section 7. The current list of Sub-processors is set out in Annex III.

7.2 Requirements for Sub-processors. INTECH Automation & Intelligence shall, prior to engaging a Sub-processor:

- carry out appropriate due diligence on the Sub-processor's ability to provide the required level of protection for Personal Data;

- impose on each Sub-processor, by written contract, data protection obligations equivalent to those imposed on INTECH Automation & Intelligence under this DPA, including in particular providing sufficient guarantees to implement appropriate technical and organisational measures such that the processing will meet the requirements of GDPR Art. 28(4);
- ensure that Sub-processor agreements include audit rights, security requirements, sub-contracting restrictions, confidentiality obligations, and data subject rights cooperation.

7.3 New Sub-processors. INTECH Automation & Intelligence shall inform the Controller of any intended addition or replacement of Sub-processors by: (a) publishing an updated Annex III on the INTECH Automation & Intelligence Trust Centre (trust.empowergpt.ai); and (b) providing individual email notification to the Controller's designated data protection contact at least 30 calendar days in advance ("Notice Period").

7.4 Objection Right. During the Notice Period, the Controller may object to the new Sub-processor on reasonable grounds related to data protection. The Parties shall seek in good faith to resolve the Controller's objection. If the Parties cannot resolve the objection within 15 days of receipt, the Controller may terminate the affected Services by written notice, without penalty, within 30 days of INTECH Automation & Intelligence's notice.

7.5 Liability. INTECH Automation & Intelligence remains fully liable to the Controller for the performance of Sub-processors' obligations under this DPA. Where a Sub-processor fails to fulfil its data protection obligations, INTECH Automation & Intelligence shall remain fully liable to the Controller (Art. 28(4) GDPR).

7.6 LLM Provider Restriction (AI-Specific Clause). Large Language Model (LLM) providers listed in Annex III shall only be activated and used in connection with the Controller's data if the Controller has explicitly selected or enabled the relevant LLM provider within the platform configuration settings or through written agreement. INTECH Automation & Intelligence shall not route the Controller's Personal Data to any LLM provider not selected by the Controller, and shall provide the Controller with clear controls to enable, disable, or switch between LLM providers. Any newly added LLM provider is subject to the notice and objection procedure in Sections 7.3–7.4 irrespective of whether a general sub-processor authorisation is in place.

8. International Data Transfers

8.1 General Restriction. INTECH Automation & Intelligence shall not transfer Personal Data to a third country outside the EEA unless:

- the transfer is to a country that has received an adequacy decision from the European Commission pursuant to GDPR Art. 45;
- the transfer is subject to appropriate safeguards pursuant to GDPR Art. 46 (e.g., Standard Contractual Clauses); or
- a specific derogation in GDPR Art. 49 applies.

8.2 Standard Contractual Clauses. Where SCCs are used as the transfer mechanism: (a) INTECH Automation & Intelligence shall enter into the relevant module of the Commission Implementing Decision (EU) 2021/914 SCCs with the applicable Sub-processors; (b) where the Controller is subject to the UK GDPR, INTECH Automation & Intelligence shall execute the UK International Data Transfer Agreement (IDTA) or Addendum to EU SCCs as applicable; and (c) copies of executed SCCs shall be made available to the Controller upon written request.

9. Data Protection Impact Assessments and Prior Consultation

9.1 DPIA Support. Taking into account the nature of processing and the information available to it, INTECH Automation & Intelligence shall provide reasonable assistance to the Controller in carrying out any Data Protection Impact Assessment required by Art. 35 GDPR.

9.2 Prior Consultation. INTECH Automation & Intelligence shall assist the Controller in carrying out any prior consultation with a supervisory authority required by Art. 36 GDPR.

10. Audits and Inspections

10.1 Audit Rights. INTECH Automation & Intelligence shall make available to the Controller all information necessary to demonstrate compliance with its obligations under Art. 28 GDPR, and shall allow for and contribute to audits, including inspections, conducted by the Controller or a mandated third-party auditor.

10.2 Audit Frequency and Notice. Audits shall be conducted no more than once per calendar year unless: (a) a Personal Data Breach has occurred; (b) a supervisory authority has initiated an investigation; or (c) the Controller has reasonable documented grounds to suspect non-compliance. Controller shall provide INTECH Automation & Intelligence with at least 30 business days' prior written notice of any on-site audit.

10.4 Third-Party Certifications. INTECH Automation & Intelligence shall, on an annual basis and upon reasonable request, provide the Controller with up-to-date copies of its relevant security certifications and audit reports, including ISO 27001 certificate, SOC 2 Type II report, and any GDPR compliance assessments. Provision of such reports satisfies the Controller's right to audit for the matters covered therein, absent specific concerns.

11. Retention and Deletion of Personal Data

11.1 Retention Policy. INTECH Automation & Intelligence shall retain Personal Data only for as long as necessary to provide the Services or as required by applicable law. INTECH Automation & Intelligence shall not retain Personal Data beyond the termination of the applicable Services without the Controller's written consent, save as required by applicable EU or Member State law.

11.2 Return or Deletion. Within 30 calendar days following the termination or expiry of the MSA (or the relevant Service), or upon the Controller's earlier written request, INTECH Automation & Intelligence shall, at the Controller's election:

- return to the Controller all Personal Data in a structured, commonly used, machine-readable format (e.g., JSON or CSV); and/or
- permanently delete or destroy all Personal Data (and all copies thereof) in its possession or control, including data held by Sub-processors.

11.3 Deletion Certification. Within 14 calendar days of completing deletion, INTECH Automation & Intelligence shall provide the Controller with written certification of deletion, specifying the methods used and confirming that all Personal Data has been deleted from production systems, backups, and Sub-processor systems (to the extent technically feasible).

12. Liability and Indemnification

12.1 Controller Liability. The Controller shall indemnify and hold harmless INTECH Automation & Intelligence from and against any claims, liabilities, fines, penalties, costs, and expenses arising from: (a) Controller's breach of this DPA or Applicable Data Protection Law; (b) Controller's unlawful instructions; or (c) Controller's failure to fulfil its obligations as Data Controller under GDPR.

12.2 Processor Liability. INTECH Automation & Intelligence shall be liable for damage caused by processing where it has not complied with obligations of GDPR specifically directed at processors, or where it has acted outside or contrary to the Controller's lawful instructions, in each case in accordance with GDPR Art. 82.

12.3 Limitation of Liability. Subject to applicable law, INTECH Automation & Intelligence's total aggregate liability under this DPA (whether in contract, tort, or otherwise) shall not exceed the amounts paid by the Controller to INTECH Automation & Intelligence in the twelve (12) months preceding the claim, unless the damage results from INTECH Automation & Intelligence's gross negligence or wilful misconduct.

13. Term and Termination

13.1 Term. This DPA enters into force on the Effective Date and continues in force for the duration of the MSA, unless earlier terminated in accordance with this Section 13.

13.4 Survival. The following obligations survive termination of this DPA: confidentiality obligations (Section 3.4); return and deletion obligations (Section 11); audit rights in respect of the processing period (Section 10); liability provisions (Section 12); AI training prohibition (Section 17); and the prohibition on non-EU/EEA access without safeguards (Section 16.4) — each for a period of three (3) years following termination unless a longer period is required by applicable law.

---

14. Governing Law and Jurisdiction

14.1 Governing Law. This DPA is governed by and shall be construed in accordance with the laws of the Federal Republic of Germany, without reference to conflict of laws principles.

14.2 Jurisdiction. The Parties irrevocably submit to the exclusive jurisdiction of the courts of Munich, Germany, to settle any dispute arising out of or in connection with this DPA. Notwithstanding the foregoing, either Party may seek emergency injunctive or other equitable relief in any court of competent jurisdiction.

14.3 GDPR Supervisory Authority. INTECH Automation & Intelligence's lead supervisory authority under Art. 56 GDPR is [the Bavarian State Office for Data Protection Supervision (BayLDA)]. Controller may also lodge complaints with its competent local supervisory authority.

---

15. Miscellaneous

15.1 Entire Agreement. This DPA (together with the Annexes and the MSA) constitutes the entire agreement between the Parties relating to the processing of Personal Data and supersedes all prior understandings, representations, or agreements on that subject.

15.2 Amendments. Amendments to this DPA shall only be effective if in writing and signed by duly authorised representatives of both Parties. INTECH Automation & Intelligence may unilaterally update this DPA to reflect changes in Applicable Data Protection Law or supervisory guidance, provided INTECH Automation & Intelligence gives the Controller at least 30 calendar days' prior written notice and the Controller does not object within that period.

15.3 Severability. If any provision of this DPA is held invalid, illegal, or unenforceable, the remaining provisions shall continue in full force and effect. The Parties shall negotiate in good faith to replace any invalid provision with a valid provision achieving the closest possible economic and legal effect.

15.5 Notices. Notices under this DPA shall be given in writing (including email) to the contacts identified in Annex I. Notices to INTECH Automation & Intelligence regarding data protection shall be sent to privacy@empowergpt.ai.

15.7 Language. This DPA is executed in the English language. In the event of conflict between any translation and the English text, the English text shall prevail.

16. Logs, Access Control and Data Separation

16.1 Log Minimisation. INTECH Automation & Intelligence shall apply a principle of log minimisation, collecting and retaining only those logs that are necessary for security monitoring, audit, legal compliance, and service integrity. Log data shall not be retained for longer than necessary and shall be subject to defined retention schedules. Where technically feasible, personal data within logs shall be pseudonymised or anonymised.

16.3 Access Controls on Logs and Production Data. Access to logs and production data containing Personal Data shall be:

- strictly restricted via role-based access control (RBAC), applying least-privilege principles;
- granted only to personnel who require access for legitimate operational, security, or legal purposes;
- subject to multi-factor authentication (MFA) for all privileged access;
- logged and monitored through a centralised SIEM system, with anomalous access triggering automated alerts;
- reviewed at least quarterly, with access rights revoked promptly upon role change or departure.

16.4 Remote and Non-EU/EEA Access. Access to Personal Data or systems processing Personal Data from outside the EU/EEA shall be:

- strictly limited and granted only where operationally necessary and subject to documented justification;
- subject to the same or equivalent safeguards as in-EEA access, including encryption, MFA, and audit logging;
- documented in an access log that is available to the Controller upon request;
- treated as a Restricted Transfer where applicable and governed by appropriate transfer mechanisms under Section 8 of this DPA.

16.5 Tenant Data Separation. INTECH Automation & Intelligence shall implement strict logical separation between the Personal Data of different customers (tenants) using infrastructure-level and application-level isolation controls. The Controller's Personal Data shall at no time be accessible to or commingled with Personal Data of any other customer. Data separation controls shall be verified as part of INTECH Automation & Intelligence's annual security assessments.

17. Prohibition on Use of Personal Data for AI Training and Model Improvement

17.1 Absolute Prohibition. INTECH Automation & Intelligence shall not, under any circumstances, use Personal Data processed on behalf of the Controller for:

- training, fine-tuning, or otherwise improving any artificial intelligence, machine learning, or large language model (LLM), whether operated by INTECH Automation & Intelligence or any third party;
- creating, developing, or enhancing datasets used for AI or model development;
- benchmarking, evaluating, or testing AI models using identifiable Personal Data;
- any other purpose beyond the strict provision of the Services as described in Annex I and the MSA.

17.2 Scope — Sub-processors and LLM Providers. The prohibition in clause 17.1 applies equally to all Sub-processors, including LLM API providers. INTECH Automation & Intelligence shall contractually bind all Sub-processors, including LLM providers such as OpenAI and Anthropic, to the same prohibition. INTECH Automation & Intelligence shall verify at the time of onboarding and at least annually that such contractual prohibitions are in place and effective.

17.4 Consent Exception. Notwithstanding clause 17.1, INTECH Automation & Intelligence may use Personal Data for AI model improvement only if the Controller has provided explicit, specific, and documented prior written consent identifying the precise scope, model, purpose, and duration of such use. Any such consent may be withdrawn by the Controller at any time with immediate effect.

18. Assistance with Regulatory Compliance

18.1 General Assistance Obligation. INTECH Automation & Intelligence shall, taking into account the nature of processing and the information available to it, provide all reasonable assistance to the Controller in fulfilling its compliance obligations under Applicable Data Protection Law, beyond the specific obligations addressed in Sections 4 (Data Subject Rights), 6 (Breach Notification), and 9 (DPIAs) of this DPA.

18.2 Regulatory Enquiries and Investigations. INTECH Automation & Intelligence shall promptly notify the Controller upon receipt of any enquiry, request, inspection, or investigation by a data protection supervisory authority that relates to Personal Data processed under this DPA. INTECH Automation & Intelligence shall:

- inform the Controller within three (3) business days of receiving any such communication;
- cooperate with the Controller in preparing a coordinated response;
- not respond independently to any supervisory authority on matters relating to the Controller's Personal Data without the Controller's prior written consent, except where required to do so by law;
- provide the Controller with copies of all correspondence with supervisory authorities relating to the Controller's Personal Data, to the extent permitted by law.

Execution / Signatures

IN WITNESS WHEREOF, the authorised representatives of the Parties have executed this Data Processing Agreement as of the Effective Date.

FOR AND ON BEHALF OF	FOR AND ON BEHALF OF
INTECH Automation & Intelligence GmbH (Data Processor)	**[Client Company Name] (Data Controller)**
Signature: _____	**Signature:** _____
Name: _____	**Name:** _____
Title: _____	**Title:** _____
Date: _____	**Date:** _____

ANNEX I — Details of Processing Activities

This Annex forms part of and is subject to the DPA. It describes the subject matter, duration, nature, and purpose of the processing, the types of Personal Data, and the categories of Data Subjects as required by GDPR Art. 28(3).

Parameter	Details

Controller (Client)	[Client Company Name], [Registered Address], [Country]
Processor (INTECH Automation & Intelligence)	INTECH Automation & Intelligence GmbH, [Registered Address], Germany
Contact / DPO (Controller)	[Name, Email, Phone]
Contact / DPO (Processor)	privacy@empowergpt.ai
Processing Purpose	Provision of AI-powered enterprise knowledge management and productivity services, including: (1) enterprise document search and retrieval; (2) AI-assisted query answering and knowledge extraction; (3) AI assistant / chat interface for authorised users; (4) document ingestion, indexing, and semantic search; (5) integration with Controller's internal systems (e.g. SharePoint, Google Drive, Confluence, CRM); (6) processing of user prompts and generation of AI responses; (7) usage analytics and access logging for service integrity and security. The exact scope of active use cases shall be agreed in the MSA or a separate Statement of Work.
Legal Basis (Controller)	Art. 6(1)(b) GDPR (contract performance); Art. 6(1)(c) GDPR (legal obligation); Art. 6(1)(f) GDPR (legitimate interests) — as applicable per Controller's determination
Categories of Data Subjects	Controller's employees, contractors, and authorised users of the INTECH Automation & Intelligence platform; individuals referenced within documents, communications, or other content uploaded by the Controller or its authorised users
Categories of Personal Data	Identity data (name, username, employee ID); contact data (work email, phone); usage and interaction data (prompts, queries, AI responses, document content uploaded by users); metadata (file names, timestamps, access patterns, document properties, user activity logs); technical data (IP address, device identifiers, session logs, browser type); potentially special categories of data only if explicitly processed by the Controller within uploaded content
Special Categories	None intended; Controller is responsible for not uploading special category data unless a separate written agreement is in place
Nature of Processing	Collection, recording, organisation, structuring, storage, retrieval, use, transmission, and erasure of personal data via cloud-hosted AI services; AI-based analysis and response generation; integration with third-party systems designated by Controller
Duration of Processing	For the term of the Master Services Agreement plus any applicable statutory retention periods; after termination per Section 11 of this DPA
Sub-processors Authorised	As listed in Annex III; Controller has granted general authorisation subject to the objection procedure in Section 7

ANNEX II — Technical and Organisational Measures (TOMs)

This Annex sets out the technical and organisational security measures implemented by INTECH Automation & Intelligence pursuant to GDPR Art. 32 and Art. 28(3)(c). These measures represent a minimum standard; INTECH Automation & Intelligence may implement additional measures from time to time.

Control Domain	Measure	Standard / Reference

Access Control	Role-based access control (RBAC) with least-privilege principle; MFA enforced for all privileged accounts; privileged access reviews quarterly Identity and authentication managed via Keycloak using OpenID Connect (OIDC); enterprise users may authenticate via external IDPs (e.g. Azure AD); three application roles (Organisation Administrator, Workspace Administrator, Regular User) and three content roles (Viewer, Contributor, Controller) with custom role support; RBAC integrated with Azure AD for Kubernetes and database access	ISO 27001 A.9; NIST AC
Encryption at Rest	AES-256 encryption for all stored personal data; key management via HSM (FIPS 140-2 Level 3) Application secrets, API keys and encryption keys stored and managed in Azure Key Vault; secrets injected into Kubernetes pods via External Secrets (never stored in environment variables or source code); Azure AD used for authentication to PostgreSQL and Azure services in lieu of static credentials; all keys stored in encrypted storage	ISO 27001 A.10; SOC 2 CC6
Encryption in Transit	TLS 1.3 enforced for all data in transit; HSTS enforced; additional application-layer AES-256 encryption of all API request/response parameters using short-lived ephemeral session keys (agreed out-of-band, never transmitted over the wire); HTTP-only, SameSite and Secure cookie attributes enforced with server-side cookie encryption; CORS restricted to trusted domains; NGINX ingress with TLS certificates managed by Cert Manager	OWASP TLS; NIST SP 800-52
Network Security	Segmented VPC architecture; WAF and DDoS protection; intrusion detection/prevention (IDS/IPS); regular vulnerability scanning Azure private endpoints for storage accounts and databases (no public internet exposure); firewall rules restricting access to specific IP ranges and trusted Azure services; service-to-service authentication; Infrastructure as Code (IaC) with mandatory peer-review pull requests	ISO 27001 A.13; CIS Controls
Logging & Monitoring	Centralised SIEM; audit logs retained ≥ 12 months; automated alerting for anomalous access patterns; tamper-evident log storage	ISO 27001 A.12; SOC 2 CC7
Incident Response	Documented IR plan; 24/7 SOC; breach notification SLA of 72 hours to Controller; annual IR simulations	ISO 27001 A.16; GDPR Art. 33
Vulnerability Management	Monthly automated scans; annual external penetration testing; critical/high patches within 30 days; SLA-tracked remediation Static code analysis integrated into CI/CD pipeline for all code changes prior to deployment; periodic security audits and penetration testing conducted by external cybersecurity specialists; file upload validation includes strict file-type checks and antivirus scanning; parameterised SQL used throughout to eliminate SQL injection risk; CSRF tokens embedded in all forms; generic error messages enforced to prevent information leakage	NIST SP 800-115; ISO 27001

Physical Security	Tier-III+ data centres; biometric + badge access; CCTV surveillance; co-location providers hold ISO 27001 certification	ISO 27001 A.11; SOC 2 A1
Business Continuity	RTO ≤ 4 hours; RPO ≤ 1 hour; geo-redundant backups; annual BCP/DR tests with documented results Automated daily backups with a 30-day secure retention period; backups encrypted at rest (AES-256) with equivalent access controls to production systems; backup access logs available to Controller on request	ISO 22301; SOC 2 A1
Employee Security	Background checks pre-employment; annual GDPR and security awareness training; NDAs for all staff with data access; disciplinary procedures	ISO 27001 A.7; GDPR Art. 28(3)(b)
AI Model Governance	No training of LLMs on Controller's personal data without explicit written consent; data isolation between tenants; model output filtering	NIST AI RMF; EU AI Act considerations
Data Minimisation	Processing limited to what is necessary for service delivery; pseudonymisation applied where feasible; retention policies enforced automatically	GDPR Art. 5(1)(c) and (e)
Sub-processor Controls	Contractual DPA with all sub-processors; annual compliance reviews; sub-processor TOMs verified at onboarding	GDPR Art. 28(4)
Pseudonymisation	User identifiers pseudonymised in analytics and logging systems; re-identification controls in place	GDPR Art. 4(5); Art. 32(1)(a)

INTECH Automation & Intelligence reviews and updates these measures at least annually and following any significant change to processing activities, security incidents, or the threat landscape. Up-to-date details are published at trust.empowergpt.ai.

ANNEX III — Authorised Sub-processors

The following Sub-processors are authorised by the Controller pursuant to Section 7 of this DPA. INTECH Automation & Intelligence maintains a live, up-to-date version of this register at trust.empowergpt.ai/sub-processors. Material changes (additions or replacements) are subject to the 30-day notice and objection procedure in Sections 7.3–7.4. Each Sub-processor has been assessed for GDPR compliance and is bound by a written DPA with INTECH Automation & Intelligence.

Sub-processor	Registered Address	Service / Purpose	Location	Transfer Basis
Microsoft Azure	Microsoft Ireland Operations Ltd, One Microsoft Place, Dublin, Ireland	Core infrastructure, compute, storage, networking. Azure OpenAI Service (LLM inference and embeddings); Azure Speech Service (voice-to-text transcription)	Germany West Central	EU adequacy; GDPR Art. 45

Google Cloud AI (via GCP)	Google Cloud EMEA Ltd, 70 Sir John Rogerson's Quay, Dublin 2, Ireland	LLM inference: Gemini models (Google) and Claude models (Anthropic, via GCP integration); prompts, responses, context data (Controller must explicitly enable)	EU region only (GCP EU deployment)	EU adequacy; GDPR Art. 45; no cross-region transfer
E2B	E2B, Inc. (vendor-managed infrastructure)	Secure sandboxed code execution environment (code interpreter); user-submitted code, execution outputs, temporary runtime data	Vendor-managed	Standard contractual protections; isolated ephemeral execution
Cloudflare	Cloudflare, Inc., 101 Townsend St, San Francisco, CA 94107, USA (EU edge PoPs)	DNS, CDN, WAF, DDoS protection; IP address and request metadata only	Global edge network	EU SCCs (Art. 46 GDPR); Cloudflare DPA
PostHog	PostHog, Inc. (EU-region deployment)	Product and usage analytics; event data and usage metadata; no AI prompt or sensitive content tracked	EU (configured deployment)	EU adequacy; GDPR-compliant setup

Notes: (1) AI / LLM subprocessors (Google Cloud AI) are inactive by default and process Controller Personal Data only once the Controller explicitly enables the relevant model via platform settings or written agreement (per Section 7.6). (2) The following components are self-hosted within INTECH Automation & Intelligence's Azure environment and are not subprocessors: Keycloak, Grafana, Prometheus, Grafana Loki. (3) Primary infrastructure region is Germany West Central (Azure). AI processing regions: Azure OpenAI → EU Data Zone; Google Cloud AI (Gemini / Claude) → EU region; Azure Speech → EU region; PostHog → EU region. (4) Data retention: Blob Storage soft-delete 95 days (versioning enabled); PostgreSQL backups 35 days; Logs 90 days; Metrics 10 days. (5) This list is reviewed and updated prior to onboarding any new subprocessor. The live version is published at trust.empowergpt.ai/sub-processors and supersedes this document after signature. (6) Registered addresses are provided for information; legal entity or address changes will be notified to the Controller. (7) Certifications and audit reports for key subprocessors are available upon written request to privacy@empowergpt.ai.

ANNEX IV — Standard Contractual Clauses and Transfer Mechanisms

A. EU Standard Contractual Clauses

Where INTECH Automation & Intelligence or any Sub-processor transfers Personal Data to a third country without an EU adequacy decision, the transfer shall be subject to the Standard Contractual Clauses adopted under Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (the "EU SCCs").

For transfers from the Controller (as data exporter) to INTECH Automation & Intelligence (as data importer) outside the EEA, the Module Two (Controller-to-Processor) SCCs shall apply, and the following selections are made: