Data Processing Agreement (DPA)

Effective 01.01.2025 · Version 1.0

Flinker GmbH

Preamble

Between: Flinker GmbH, Zittelstraße 7, 80796 Munich, Germany, Amtsgericht München HRB 254870 (hereinafter "Processor")

and: the customer identified in the Main Contract (hereinafter "Controller")

together: "the Parties"

This Data Processing Agreement (DPA) is incorporated into and forms part of the Main Contract (Subscription Agreement or Order Form) between the Parties and becomes effective upon execution of the Main Contract.

1.1 This DPA governs the processing of personal data by the Processor on behalf of the Controller pursuant to Art. 28 GDPR.

1.2 The subject matter is the operation of Flinker's Microsoft 365-native SaaS applications (IFC Viewer for SharePoint, Teams, Excel, Power BI; SharePoint CDE; Copilot for IFC; SharePoint Protect) used by the Controller under the Main Contract.

1.3 This DPA runs for the duration of the Main Contract and terminates automatically upon its termination, subject to any continuing obligations under § 13.

§ 2 Nature and Purpose of Processing

2.1 Nature: Collection, storage, use, and deletion of personal data to the extent strictly necessary for the provision of the contracted services.

2.2 Purpose:

Authentication and authorisation of users against the Controller's Microsoft 365 tenant

Operation and provision of Flinker applications

Support and consulting services upon request of the Controller

Anonymised usage analytics for product improvement

2.3 Architecture note: Flinker applications run as SPFx web parts entirely within the Controller's Microsoft 365 tenant. IFC files, BIM models, and project data never leave the Controller's tenant at any time. Viewer source code is delivered as static assets via Azure CDN; no content data is transferred in this process.

Exception — Copilot for IFC: IFC files are processed exclusively in the user's browser. Only chat text (user inputs and AI responses) is transmitted to Microsoft Azure AI (Azure OpenAI Service). No IFC file content leaves the browser.

§ 3 Categories of Personal Data and Data Subjects

Data categories processed

Microsoft 365 Tenant ID: Required for authentication and licence verification. Does not directly identify a natural person but enables attribution to the Controller's tenant.

User email address (optional): Collected only in connection with support requests or where explicitly provided during login. Not collected by default.

Anonymised usage metrics: Aggregated, non-personal data on usage intensity (e.g. file types opened). No inference to natural persons possible.

Chat inputs — Copilot for IFC only: Text-based user inputs in the Copilot interface. Processed via Microsoft Azure AI. No IFC file content.

Categories of data subjects

IT administrators and tenant administrators of the Controller

End users (employees) of the Controller, to the extent they actively use Flinker applications and engage optional features involving personal data

§ 4 Obligations of the Processor

4.1 The Processor processes personal data only on documented instructions from the Controller (§ 6), unless required to do so by applicable Union or Member State law. In such cases, the Processor shall inform the Controller prior to processing, unless prohibited by law.

4.2 The Processor ensures that all persons authorised to process personal data are subject to appropriate obligations of confidentiality, whether by contract or by operation of law.

4.3 The Processor implements the technical and organisational measures described in § 8.

4.4 The Processor assists the Controller, by appropriate technical and organisational means, in fulfilling obligations to respond to data subject requests under Art. 15–22 GDPR, and in fulfilling obligations under Art. 32–36 GDPR (security, breach notification, DPIA, prior consultation).

4.5 Data protection contact for the Processor: privacy@flinker.app

§ 5 Obligations of the Controller

5.1 The Controller is solely responsible for the lawfulness of the processing and for compliance with applicable data protection law within its sphere of responsibility.

5.2 The Controller shall issue all instructions in writing or in a documented electronic format.

5.3 The Controller warrants that it is duly entitled to transfer the personal data to the Processor.

5.4 The Controller shall notify the Processor without undue delay upon identifying errors or irregularities in the Processor's processing activities.

§ 6 Instructions

6.1 The Processor processes personal data only on documented instructions from the Controller. The Main Contract and any Statements of Work (SOW) constitute the initial instructions.

6.2 Instructions may be issued in writing or by email to: privacy@flinker.app

6.3 If the Processor considers an instruction to be unlawful, it shall notify the Controller without undue delay. The Processor is entitled to suspend execution until the Controller confirms or withdraws the instruction.

§ 7 Confidentiality

The Processor contractually or by operation of law binds all employees and service providers who have access to the Controller's personal data to appropriate confidentiality obligations. These obligations survive the termination of the relevant employment or service relationship.

§ 8 Technical and Organisational Measures (TOMs)

Pseudonymisation and encryption

Pseudonymisation of personal data where technically feasible and proportionate

Encryption of all systems storing or processing personal data

Secure data transmission exclusively via HTTPS (TLS 1.2 or higher)

Confidentiality and integrity

Exclusive use of Microsoft Azure infrastructure with EU data centres (primary: Germany, Ireland)

Access to the production environment restricted to a small number of authorised employees based in Germany

Azure Active Directory for authentication and identity management; tenant isolation via multi-tenancy

No proprietary authentication provider — exclusively Microsoft token-based authentication

SPFx web parts execute JavaScript exclusively in the user's browser; no server-side code execution in the customer's tenant

Azure Authentication Log for access control and monitoring

Availability and resilience

Regular data backups provided by Microsoft Azure

Monitoring and logging via Azure Log Analytics

Incident management via Microsoft Azure (release management, backup, rapid recovery)

Option for complete self-hosting within the customer's own Azure tenant

Review and evaluation

Internal control system for regular review and updating of TOMs

Code reviews, functional and integration testing incorporating security requirements

Agile change management with automated and manual tests prior to each deployment

Information Security Management System (ISMS) via Microsoft Data Governance

§ 9 Sub-processors

9.1 The Controller hereby grants general authorisation for the Processor to engage the sub-processors listed below. The Processor shall notify the Controller of any planned changes (addition or replacement of sub-processors) at least 30 days in advance. The Controller may object to any such change on substantiated data protection grounds by written notice within that period.

9.2 Approved sub-processors:

Provider	Purpose	Location	Products
Microsoft Corporation	Cloud infrastructure (Azure), CDN, authentication (Azure AD), AI processing (Azure OpenAI Service)	EU — Germany, Ireland	All products; Azure OpenAI Service only for Copilot for IFC

§ 10 Assistance with Data Subject Rights

The Processor assists the Controller, through appropriate technical and organisational measures, in responding to requests from data subjects exercising their rights under Art. 15–22 GDPR (access, rectification, erasure, restriction, portability, objection). Erasure requests are fulfilled by the Processor at no additional charge.

§ 11 Personal Data Breach Notification

11.1 The Processor shall notify the Controller of any identified personal data breach without undue delay, and no later than 36 hours after becoming aware, by email to the contact address provided by the Controller.

11.2 The notification shall include, to the extent known: the nature of the breach; the categories and estimated number of data subjects and records affected; the likely consequences; the remedial measures taken or planned; and a contact person at the Processor.

11.3 As the Processor does not operate its own authentication infrastructure and relies entirely on Microsoft Azure, a security incident can only arise through Microsoft Azure infrastructure. The Processor shall notify the Controller immediately upon becoming aware of any such incident.

§ 12 Audit Rights and Evidence of Compliance

12.1 The Processor makes available to the Controller all information necessary to demonstrate compliance with the obligations set out in Art. 28 GDPR.

12.2 The Processor allows audits and inspections by the Controller or an auditor mandated by the Controller. Audits must be announced in writing with at least 14 days' notice, conducted during normal business hours, and limited in scope to data protection-relevant aspects of the processing activities. The Controller bears all associated costs.

12.3 For audits of Microsoft infrastructure, the Controller is referred directly to Microsoft. The Processor has no access to Microsoft data centres beyond the publicly available certifications and Trust Centre documentation.

§ 13 Deletion and Return of Data upon Termination

13.1 Upon termination of the Main Contract, the Processor shall delete all personal data of the Controller without undue delay, unless a statutory retention obligation requires continued storage.

13.2 As Flinker applications run within the Controller's own Microsoft 365 tenant, and IFC files and project data never leave the tenant, the deletion of those assets is entirely within the Controller's responsibility. The Processor deletes only data stored on Processor infrastructure: Tenant ID, optional email address, and usage metrics.

13.3 Upon written request, the Processor provides written confirmation of deletion.

§ 14 Transfers to Third Countries

14.1 Processing by the Processor and its approved sub-processor Microsoft takes place on servers within the European Union (data centres in Germany and Ireland).

14.2 To the extent that Microsoft Corporation, headquartered in the United States, acts as a sub-processor, any third-country transfer is based on the EU–U.S. Data Privacy Framework (adequacy decision of the European Commission of 10 July 2023) and on Standard Contractual Clauses (SCC) pursuant to Implementing Decision 2021/914/EU.

14.3 The Processor does not transfer personal data to third countries other than as described in § 14.2.

§ 15 Final Provisions

15.1 This DPA forms part of the Main Contract and is supplemented by it. In the event of conflict, this DPA prevails with respect to data protection matters.

15.2 Amendments to this DPA require written form or a documented electronic agreement signed by both Parties.

15.3 This DPA is governed by the laws of the Federal Republic of Germany. The exclusive place of jurisdiction for all disputes arising from this DPA is Munich, to the extent permitted by applicable law.

15.4 Should any provision of this DPA be or become invalid or unenforceable, this shall not affect the validity of the remaining provisions.

15.5 This DPA becomes effective upon execution of the Main Contract or, for Enterprise customers requiring a countersigned copy, upon separate execution of the downloadable .docx version.

EXECUTION

By signing below, both Parties agree to the terms of this Data Processing Agreement.

Controller (to be completed by customer)	**Processor** Flinker GmbH, Munich
Signature	Signature
Name (print)	Name (print)
Title / Role	Title / Role
Date	Date