



Data Processing Agreement (DPA)

Effective 2026-11-15 · Version 2026-11

Flinker GmbH

Preamble	3
§ 1 Subject Matter, Scope and Duration	3
§ 2 Nature and Purpose of Processing	3
§ 3 Categories of Personal Data and Data Subjects	4
Data categories processed	4
Categories of data subjects	5
§ 4 Obligations of the Processor	5
§ 5 Obligations of the Controller	5
§ 6 Instructions	6
§ 7 Confidentiality	6
§ 8 Technical and Organisational Measures (TOMs)	6
Pseudonymisation and encryption	6
Confidentiality and integrity	6
Availability and resilience	6
Review and evaluation	7
§ 9 Sub-processors	7
§ 10 Assistance with Data Subject Rights	8
§ 11 Personal Data Breach Notification	9
§ 12 Audit Rights and Evidence of Compliance	9
§ 13 Deletion and Return of Data upon Termination	9
§ 14 Transfers to Third Countries	9
§ 15 Final Provisions	10
EXECUTION	10

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, Order Form, or the Flinker Terms and Conditions accepted when obtaining Flinker applications, e.g. via Microsoft AppSource / Microsoft Marketplace or online checkout) between the Parties and becomes effective upon conclusion of the Main Contract.

§ 1 Subject Matter, Scope and Duration

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 provision of Flinker's Microsoft 365 applications (including IFC Viewer for SharePoint, Teams, Excel, Power BI; Power BI Data Connector; SharePoint CDE / ISO 19650; SharePoint Protect; Copilot for IFC) and of related licensing, support, implementation and consulting services 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.

1.4 Enterprise configurations: Under an Enterprise agreement, the Parties may agree on a deviating deployment, e.g. self-hosting of the applications or backend in the Controller's own Azure tenant (including container deployment), use of other Azure regions, use of the Controller's own Azure AI resources for Copilot for IFC, version pinning, or delivery of all assets from the Controller's environment. The agreed configuration is documented in the Order Form or Statement of Work and takes precedence over the corresponding descriptions in §§ 2, 3, 8, 9 and 14. Where processing takes place exclusively in the Controller's environment without access by the Processor, the Processor does not act as a processor in this respect.

§ 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

Licence verification and anonymisation of usage data for statistical purposes (see 2.4)

2.3 Architecture note: Flinker applications run as SPFx web parts, Teams apps, Office add-ins or Power BI visuals within the Controller's Microsoft 365 environment, or as web and desktop viewers; files are parsed and rendered locally in the user's browser or application. IFC files, BIM models, and project documents are not uploaded to, stored on or mirrored on Processor infrastructure. Viewer source code is delivered as static assets via the Processor's Azure CDN (third-party libraries and fonts: see § 9.4); no content data is transferred in this process. Exceptions are limited to Copilot for IFC (below) and the optional map context (§ 9.3).

Exception — Copilot for IFC: IFC files are processed in the user's browser and are not transmitted as files. Chat inputs, AI responses and the element data a query refers to (e.g. property values of the elements concerned) are transmitted, together with the user's email address where available, via the Processor's Azure environment to Microsoft Azure OpenAI Service. The Azure OpenAI resource is located in Sweden Central (EU); as a global deployment, inference may take place in Azure regions outside the EU (see § 14). Requests are processed transiently and not retained by the Processor; Microsoft may retain prompts and responses for up to 30 days for abuse monitoring. Where Copilot for IFC is operated with the Controller's own Azure AI resources (Enterprise), prompts and results remain within the Controller's environment and are not processed by the Processor.

2.4 Processor's own purposes: Usage data is anonymised by the Processor on the Controller's instruction; anonymised data is not personal data and may be used by the Processor for statistics and product improvement. Contract, account and billing data of the Controller (including invoicing and payment processing) is processed by the Processor as an independent controller and is not subject to this DPA.

§ 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 identifiers: User principal name (UPN) or email address of the signed-in user, transmitted automatically depending on the application (e.g. when the SharePoint, Teams, web or Excel viewer starts, during licence checks and with Copilot requests; for Power BI only the licence email address stored by the Controller); names and email addresses provided in connection with support requests.

Technical and usage data: Integration data (application, host, client, version, AppSource plan), timestamps, IP addresses (connection logs) and usage events (e.g. file types opened); pseudonymised where technically feasible and anonymised for statistical purposes (see 2.4).

Copilot for IFC (unless operated with the Controller's own Azure AI resources): Chat inputs, AI responses and the element data a query refers to (see 2.3). May contain personal data where users enter it or where it is contained in model properties (e.g. names of authors or responsible persons). No IFC files are transmitted.

Support data: Personal data contained in content that the Controller makes available in the course of support, implementation or consulting services (e.g. via screen sharing, guest access to the Controller's tenant or files provided for troubleshooting).

Categories of data subjects

IT administrators and tenant administrators of the Controller

End users of the Controller (employees as well as guest users and external collaborators authorised by the Controller), to the extent they actively use Flinker applications and engage optional features involving personal data

Persons named in content processed under § 3 (support data, Copilot queries), e.g. authors or contact persons in models, documents or issues

§ 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

Processor backend and CDN hosted exclusively on Microsoft Azure infrastructure with EU data centres (Germany, Ireland, Sweden)

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

Microsoft Entra ID (formerly Azure Active Directory) for authentication and identity management; logical separation of customer data by Tenant ID

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 response process of the Processor; backup and rapid recovery capabilities of Microsoft Azure

Option for complete self-hosting within the customer's own Azure tenant (customer build, including version pinning)

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

Hosting on Microsoft Azure infrastructure certified to ISO/IEC 27001, ISO/IEC 27018 and SOC 2 (certifications held by Microsoft)

§ 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 Ireland Operations Ltd., Dublin (Microsoft group)	Cloud infrastructure (Azure), CDN, authentication (Entra ID), AI processing (Azure OpenAI Service), map services (Azure Maps)	EU — Germany, Ireland, Sweden; Azure OpenAI inference: global	All products; Azure OpenAI Service only for Copilot for IFC; Azure Maps only for map context
Stripe Payments Europe, Ltd., Dublin	Licence verification (customer lookup by user email address or email domain) and subscription management	EU — Ireland; transfers to Stripe, Inc. (USA)	All applications with licence check

Provider	Purpose	Location	Products
Cesium GS, Inc., Philadelphia (Bentley Systems group)	Streaming of 3D map tiles (Cesium ion)	USA	IFC Viewer map context — current release only; replaced by Azure Maps with the next release
Google Ireland Limited, Dublin	Photorealistic 3D map tiles	EU / global; transfers to Google LLC (USA)	IFC Viewer map context — current release only; replaced by Azure Maps with the next release

9.3 Map context: When a user activates the optional map context, the user's browser requests map tiles directly from the map services listed above. This transmits the user's IP address and the requested map area (derived from the model's georeference); no model content is transmitted. The Controller may prevent these requests by blocking the respective endpoints; core viewing functions remain available.

9.4 Third-party resources: Depending on the application and release, the user's browser loads static open-source libraries, decoders, fonts or reference data from public content delivery networks (currently jsDelivr, unpkg, Google Fonts / gstatic, SheetJS CDN, Tailwind CDN and cdn.proj.org) and from Microsoft (Office.js, Fluent UI). In this process, the user's IP address and browser information are transmitted to the respective provider; no user identifiers, customer content or project data are transmitted.

9.5 The Processor shall bind each sub-processor by contract to data protection obligations meeting the requirements of Art. 28(3) GDPR. Where a sub-processor fails to fulfil its data protection obligations, the Processor remains fully liable to the Controller for the performance of that sub-processor's obligations (Art. 28(4) GDPR).

§ 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 These obligations also apply to personal data breaches at sub-processors, including Microsoft Azure, of which the Processor becomes aware.

§ 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, at the Controller's choice, return or delete all personal data processed on behalf of the Controller without undue delay, unless Union or Member State law requires storage of the personal data.

13.2 As Flinker applications run within the Controller's own Microsoft 365 tenant, and IFC files and project data are not stored on Processor infrastructure, the deletion of those assets is entirely within the Controller's responsibility. The Processor deletes only data stored on Processor infrastructure: Tenant ID, user identifiers, technical and usage data, and support data.

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

§ 14 Transfers to Third Countries

14.1 Processing by the Processor and Microsoft as its primary sub-processor takes place on servers within the European Union (data centres in Germany, Ireland and Sweden). Exception: inference for

Copilot for IFC runs on a global Azure OpenAI deployment and may take place in Azure regions outside the EU.

14.2 To the extent that personal data is transferred to sub-processors or their affiliates outside the EU/EEA (in particular Microsoft Corporation, Stripe, Inc., Cesium GS, Inc. and Google LLC in the United States), any such 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 this § 14 and in § 9.4.

§ 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 conclusion of the Main Contract or, for customers requiring a countersigned copy, upon separate execution of this DPA.

15.6 Liability: The limitations of liability agreed in the Main Contract also apply to this DPA. Liability towards data subjects under Art. 82 GDPR remains unaffected.

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