AXION PRIVACY POLICY

ENGLISH PUBLIC VERSION — v1.0

1. Introduction, Controller and Scope of this Privacy Policy

1.1. Purpose of this Privacy Policy

This Privacy Policy (“Privacy Policy”) explains what personal data may be processed in connection with the provision of the Axion service, the purposes and legal bases for such processing, who may have access to personal data, which processors and other recipients may participate in the processing, how long the data may be retained, and what rights are available to data subjects.

This Privacy Policy is also intended to provide transparent information about the processing of personal data associated with Axion’s operation based on artificial intelligence, model orchestration, external technology providers, integrations, code-execution environments and other technical environments.

This Privacy Policy provides, in particular, the information required under Regulation (EU) 2016/679 of the European Parliament and of the Council (“GDPR”) and other applicable data protection laws.

1.2. The Controller

The operator of the Axion service and, with respect to the processing activities falling within the scope of this Privacy Policy, except as otherwise specified in this Privacy Policy, the controller is:

Leiter Miklós Patrik
Registered office: 4090 Polgár Hunyadi utca 3.
Registration number / sole trader registration number: 62674771

Tax number: 92281868-1-29

E-mail: support@axionaiapp.com
Website: https://axionaiapp.com

(hereinafter: “Axion”, the “Controller” or the “Service Provider”).

In its capacity as controller, Axion determines the purposes and essential means of the processing of personal data carried out for the provision, operation, security, administration and development of its own service.

1.3. Scope of this Privacy Policy

This Privacy Policy applies to processing of personal data carried out by Axion in its capacity as controller.

This may include, in particular, the processing of personal data in connection with:
a) creating and managing an Axion Account;
b) identifying and authenticating the User;
c) providing Axion services;
d) operating Chat and other User interactions;
e) handling Inputs, Outputs, Artifacts, Projects and other User Content;
f) operating artificial intelligence models and orchestration processes;
g) processing files, documents, images and other content;
h) providing web search, information retrieval and related functionality;
i) operating Axion Forge, Workflow, sandbox and other execution environments;
j) operating Connected Accounts, Connected Services, integrations and Actions;

k) managing Axion Coin, purchases and related settlement processes;
l) support and complaint handling;
m) maintaining service security and preventing and investigating abuse;
n) processing technical, security and audit logs;
o) analysing service operation and, subject to applicable rules, providing analytics functionality; and
p) complying with legal and administrative obligations related to the operation of Axion.

The detailed purposes and legal bases of individual processing activities, the categories of personal data concerned, recipients and retention periods are specified in the subsequent sections of this Privacy Policy.

1.4. Axion as Controller

As a general rule, Axion acts as controller where it determines the purposes and essential means of processing personal data in connection with the operation of the Axion service itself.

This may include, in particular, processing necessary for Account operation, authentication, service provision, security, Coin settlement, support, legal compliance and administration of Axion's own operations.

Whether Axion acts as controller in relation to a particular processing operation does not depend solely on the technology used or the location where the data is stored, but also on who actually determines the purposes and essential means of the relevant processing.

1.5. Axion as Processor

In certain cases, Axion may process personal data not for its own processing purposes but on behalf of, and on the instructions of, a User.

This may occur in particular where a User processes personal data of third parties for the User's own purposes through an application, software, workflow, automation or other system created, modified or deployed with Axion, or operated on infrastructure provided by Axion.

Where the User determines the purposes and essential means of processing personal data and Axion processes such personal data on behalf of and in accordance with the User's instructions, the User will, as a general rule, qualify as the controller in respect of that processing and Axion will act as processor.

Processing carried out by Axion as processor may be subject to separate data processing terms, a Data Processing Agreement, or other contractual provisions compliant with Article 28 GDPR.

This Privacy Policy primarily provides information about processing carried out by Axion as controller and does not, by itself, replace any data processing agreement applicable to Axion's activities as processor.

1.6. User-Operated Applications and Systems

Axion may enable the creation, modification, deployment or operation of applications, websites, program code, workflows, automations, services and other software systems.

The fact that an application or other system has been created, modified or deployed in whole or in part using Axion, or is operated on Axion's technical infrastructure, does not in itself mean that Axion becomes the controller of personal data processed by that application.

If the User determines what personal data the User-operated application collects or processes, from whom it collects data, for what purposes it processes such data, how the data is used, to whom it is disclosed or made available, how long it is retained, or what functionality is provided to the User's own users, then, as a general rule, the User is responsible for compliance with the applicable data protection requirements arising from such processing.

This may include, in particular, ensuring an appropriate legal basis, providing appropriate information to data subjects, enabling data subject rights, obtaining any required consents, determining retention rules, implementing appropriate access controls and security measures, and complying with applicable data protection laws.

Where Axion infrastructure processes personal data on behalf of the User in the course of operating such an application, Axion may act as processor in respect of that processing.

Axion's role as processor in such circumstances does not make Axion the party determining the purposes of the processing carried out by the application and does not transfer the User's obligations as controller to Axion.

Axion may, however, act as an independent controller in respect of separate processing activities associated with the operation of such an application where Axion itself determines the purposes and essential means, for example for its own Account administration, security logging, abuse prevention, billing or compliance with legal obligations.

The controller and processor roles must therefore be determined in each case by reference to the specific processing operation concerned.

1.7. Processors, Technology Providers and Third Parties

Axion may use external technology and infrastructure providers to operate its services.

Depending on the circumstances of the relevant processing, the applicable contractual terms and applicable law, such providers may act as processors, sub-processors or, in relation to certain separate processing activities, as independent controllers.

Technology providers used by Axion may include, in particular, providers of artificial intelligence models, cloud and database infrastructure, search services, document processing and OCR services, media and file management services, sandbox and code-execution services, and analytics services.

Axion does not necessarily disclose all personal data to every technology provider.

Based on Axion's orchestration, routing and technical processes, only those providers necessary for the performance of a particular task may participate in that task, and only data necessary for, or related to, the relevant operation may be transmitted or made accessible to the relevant provider, in accordance with Axion's technical operation and applicable requirements.

Further provisions of this Privacy Policy set out more detailed rules concerning processors, recipients, international data transfers and the roles of individual technology providers.

1.8. Access by Axion Personnel

Internal access to personal data is not unrestricted.

Axion personnel with access to personal data may access such data only to the extent appropriately justified and necessary for the performance of the relevant task.

Such access may occur, in particular, for support, investigation of security incidents, prevention or investigation of abuse, remediation of technical errors, compliance with legal obligations, or another appropriately justified operational purpose.

The technical ability to access personal data does not, in itself, mean that an Axion staff member is authorised to view or use the data for any purpose.

Axion restricts internal access through technical and organisational measures appropriate to the size, operation and risks of the service.

1.9. Third-Party Services

Certain Axion features may allow the User to connect a service, account, application or system operated by a third party to Axion.

In the course of operating such a Connected Service or other external service, the relevant third party may also act as an independent controller in relation to its own processing purposes.

The third party's own privacy notice and terms may also apply to processing carried out in connection with its own service.

This Privacy Policy does not govern processing carried out by a third party for its own purposes where Axion does not determine the purposes and means of that processing.

However, where Axion retrieves, uses or transmits data from a Connected Service at the User's request for the purpose of operating the Axion service, the relevant provisions of this Privacy Policy apply to the processing carried out by Axion.

1.10. Google Authentication and Connected Google Services

Axion may allow registration or sign-in through a Google Account.

Authentication through a Google Account is not the same as connecting additional services provided by Google—such as Gmail, Google Drive, Google Calendar or another Google service—to Axion.

During registration and sign-in, Axion requests access only to Google Account data necessary or appropriate for creating, identifying and authenticating the Account or for the relevant functionality.

If the User subsequently connects an additional Google service to Axion, Axion may request separate access permissions required for the relevant integration.

Such access, the permission scopes used, the processing of data accessible through Google APIs, the handling of access tokens and termination of the connection are governed by the provisions of this Privacy Policy relating to Connected Accounts and integrations.

1.11. Relationship of this Privacy Policy to Other Axion Documents

This Privacy Policy is Axion's data protection information document and primarily provides information about the processing of personal data.

The contractual terms governing the use of Axion are set out in the Terms of Service.

The rules governing permitted and prohibited use of Axion are set out in the Acceptable Use Policy, which forms part of the Terms of Service.

Detailed rules concerning cookies, similar technologies and related processing are set out in the Cookie Notice.

Further information concerning the operation of Axion's artificial intelligence systems, AI-generated content and applicable transparency information may be provided in a separate AI Transparency Notice.

Further information concerning Axion's approach to security may be provided in the Security Overview.

Where Axion acts as processor on behalf of a User, such processing may be subject to a separate Data Processing Agreement or Data Processing Terms.

Acknowledging or reviewing this Privacy Policy does not, in itself, constitute general consent to the processing of personal data.

Axion carries out each personal-data processing operation on the legal basis appropriate to that processing and specified in this Privacy Policy.

2. Categories and Sources of Personal Data

2.1. Általános elvek és adatforrások

Axion által kezelt personal data köre attól függ, hogy the User mely functionkat ifsználja, milyen content ad meg, milyen integrációkat kapcsol össze, and milyen műveleteket végez a Serviceban. Nem minden, e fejezetben felsorolt adatkategória is kezelandre minden Felifsználó in the case of.

A personal data may originatenak directly the Usertól; provided by the User uploaded vagy created contentból; provided by the User összekapcsolt external Serviceokból; az Axion technical rendszereiből and infrastruktúrájából; external vagy publican accessible sourceokból; and az AI-, orchestration-, research- vagy más feldolgozási műveletek in the course of létrejövő resultekből and metadatából.

Axion a personal data processing az adott function, feladat, security vagy jogi cél szempontjából necessary and releváns datara korlátozza.

2.2. Account-, profil- és hitelesítési adatok

Axion Account creationa, processing and the User authenticatione in the course of may process in particular nevet vagy megjelenített nevet, e-mail-címet, belső Account- and User-identifierkat, profilimageet vagy avatarra relating to data, nyelvi and felifsználói beállításokat, Account statust, and a regisztrációhoz and jogi documentokhoz related esemény- and verziódataat.

Google vagy más támogatott external authenticationi szolgáltató ifsználata esetén may processjük a authenticationhez necessary provider-identifierkat, OAuth- vagy ifsonló authenticationi metadataat, and a bejelentkezandi and munkamenet-security dataat.

2.3. Felhasználói tartalom, fájlok, Outputok, Artifacts és Projects

Axion ifsználata in the course of provided by the User provided vagy created content personal data may contain. Ide tartozift in particular a Cift and más Input tartalma, promptok, utasítások, üzenetek, uploaded fileok and documentok, azok neve, formátuma, metaadatai and feldolgozott vagy OCR-rel kinyert tartalma.

Személyes adat jelenhet meg az Axion által created Outputokban, összefoglalókban, elemzandekben, kódban, documentokban and más resultekben, further az Artifacts and Projects tartalmában, verzióiban, related metaadataiban and provenance-információiban.

Axion nem feltételezi, hogy minden Felifsználói content personal data tartalmaz; a tényleges adatkör provided by the User provided vagy a feladat végreifjtása in the course of létrejövő contenttól függ.

2.4. AI-, orchestration-, research- és feladatvégrehajtási adatok

Axion AI- and orchestration-rendszere a feladat teljesítandéhez related personal data tartalmazó technical vagy tartalmi dataat is may process. Ide tartoziftnak in particular a feladatleírások, routing- and modellválasztási információk, feladatlépandek, tool- vagy agent-műveletek, köztes resultek, végreifjtási állapotok, hibák and más, a feladat koordinálásához necessary metadata.

Webes keresand, research vagy external source ifsználata esetén az Axion a keresandi lekérdezandt, a találatokból vagy más sourceból származó releváns information, source- and hivatkozási dataat, and a kutatási result

összeállításához necessary dataat may processi. Külső vagy public sourceból származó információ termandzetes személyre relating to personal data is may contain.

Kód-, Forge-, Workflow-, sandbox- vagy más végreifjtási function ifsználatakor may process programkódot, konfigurációt, futási inputot and outputot, technical logokat, hibaüzeneteket, környezeti and végreifjtási metadataat.

2.5. Connected Services, integrációk és Actions adatai

If the User external Servicet vagy Connected Accountot kapcsol az Axionhoz, may processjük az integráció identificationához necessary account- and provider-dataat, engedélyezett scope-okat and jogosultságokat, tokeneket vagy más authorization dataat, and az adott Felifsználói kérand teljesítandéhez a external Serviceból lekért vagy oda továbbított dataat.

Axion által kezdeményezett vagy támogatott Actionök esetén may processjük a művelet típusát, célrendszerét, a művelethez necessary dataat, provided by the User adott confirmation vagy jóváifgyás tényét and idejét, and a végreifjtás állapotát and resultét.

A Connected Service összekapcsolása nem jelenti azt, hogy az Axion automatikusan hozzáfér a external account valamennyi adatához. A tényleges hozzáférandt az engedélyezett scope, a provider technical működande and provided by the User kezdeményezett művelet iftározza meg.

2.6. Technikai, eszköz-, biztonsági és naplóadatok

Axion a Service operation, biztonsága, hibakeresande, abuse- and fraud-prevention, and infrastruktúra-védelem in order to technical and logdataat may process.

Ilyen adat may be in particular az IP-cím, időbélyeg, session- and request-identifier, böngandzőre vagy eszközre relating to technical információ, hálózati and rendszer-metaadat, endpoint- and műveleti információ, authentication- and security event, hibakód, teljesítményadat, and audit- vagy security logbejegyzand.

Axion törekszik arra, hogy a technical logkba ne isjön több Felifsználói content vagy érzékeny adat, mint amennyi az adott technical vagy security célhoz necessary.

2.7. Coin, Purchase, Billing and Transaction Data

Axion Coin-rendszerének, vásárlásoknak and related pénzügyi folyamatoknak a operation in the course of may process in particular Coin-egyenlegre, Coin-vásárlásra and felifsználásra, csomagra vagy termékre, amountre, currencyre, tranzakciós identifierra, statusra, timestampra, billingra and refundre relating to dataat.

Az online fizetandek feldolgozását Stripe végzi. Axion does not store teljes bankkártyaszámot, CVC/CVV-kódot vagy más teljes fizetandikártya-authenticationi data. Axion a Stripe-tól a tranzakció and a related Service kezelandéhez necessary korlátozott dataat kapift, for example fizetandi statust, tranzakció- vagy referenciaidentifiert, amountet, currencyet, refundre, cifrgebackre vagy más related tranzakciós eseményre relating to information.

A számlakiállításhoz necessary dataat az Axion a Számlázz.hu rendszerének továbbítiftja. A kiállított számlák and azok related billingi nyilvántartása a Számlázz.hu system is kezelandre and retentionre az alkalmazandó számviteli, adózási and más jogszabályi követelmények in accordance with.

2.8. Support, Communication and Analytics Data

If the User kapcsolatba lép az Axionnal, support- vagy más megkeresandt küld, may processjük a kapcsolattartási dataat, az üzenet and a related kommunikáció tartalmát, a support case identifierit, technical diagnosztikai information, csatolmányokat, and a megkeresand kezelandéhez necessary Account- vagy eseménydataat.

Ahol az Axion analitikai vagy ifsonló mérandi technológiát alkalmaz, may process a Service ifsználatára, oldal- vagy functioninterakciókra, sessionre, technical környezetre and eseményekre relating to dataat. A cookie-k and

ifsonló technológiák randzletes szabályait a Cookie Tájékoztató and jelen Tájékoztató relating to sectioni tartalmazzák.

2.9. Különleges adatok és más személyek adatai

Axion Account creationához and általános ifsználatához főszabály in accordance with nincs szükség a GDPR 9. cikke in accordance withi különleges personal data megadására. The User által biztosított content, document, Connected Service adat vagy más Input azonban ilyen data is may contain.

The Useri content más termandzetes személyek personal dataait is may containja, for example munkavállalók, ügyfelek, üzleti partnerek, címzettek, documentokban szereplő személyek vagy más ifrmadik felek adatait.

If the User más személy personal dataát dolgoztatja fel az Axionnal, az adott processingi helyzettől függően the User felelhet a appropriate legal basis, tájékoztatás and más adatvédelmi követelmények biztosításáért. A gyermekek, különleges personal data, büntetőjogi data and third partyek adatainak randzletes szabályait a 12. fejezet sets out.

2.10. User-operated applications adatai

If egy Felifsználó saját alkalmazást, workflow-t vagy más rendszert működtet Axion technológia vagy infrastruktúra ifsználatával, az ilyen rendszer végfelifsználóira vagy más data subjectjeire relating to personal data is feldolgozásra ishetnek az Axionon keresztül.

Az ilyen processingnél az adatvédelmi szerepeket a tényleges processingi célok and lényeges eszközök on the basis of kell megiftározni. If the User iftározza meg az processing célját and lényeges eszközeit, the User adatkezelő, az Axion pedig az adott feldolgozás tekintetében adatfeldolgozó may be.

A User-operated applications randzletes controller–processor modelljét a 13. fejezet and – ahol alkalmazandó – a Data Processing Agreement / Data Processing Terms sets out.

3. Purposes and Legal Bases of Processing

3.1. General Principles on Legal Bases

Axion processes personal data only for specified, explicit and legitimate purposes and assigns an appropriate legal basis under applicable data protection law to each processing activity.

Under the GDPR, Axion's processing may in particular be based on the data subject's consent [Article 6(1)(a) GDPR], performance of a contract or steps taken prior to entering into a contract [Article 6(1)(b)], compliance with a legal obligation [Article 6(1)(c)], protection of vital interests [Article 6(1)(d)], performance of a task carried out in the public interest or in the exercise of official authority [Article 6(1)(e)], or the legitimate interests pursued by Axion or a third party [Article 6(1)(f)], where the conditions of the relevant legal basis are in fact satisfied.

The same personal data may be processed for different purposes on different legal bases. Axion does not treat the existence of a legal basis for one purpose as automatic authorisation to process the data for another purpose.

3.2. Account, Authentication and Contract Administration

As a general rule, Axion processes personal data necessary to create an Account, authenticate the User, provide access, manage Account settings and administer Axion's contractual service for the performance of a contract or in order to take steps prior to entering into a contract.

Documenting the acceptance, version and date of legal documents, and maintaining certain Account and contractual records, may also be necessary for compliance with a legal obligation or on the basis of Axion's legitimate interests, in particular to demonstrate the contractual relationship, compliance and legal claims.

3.3. Provision of the Axion Service, AI Orchestration and Performance of Tasks

As a general rule, Axion processes personal data necessary to operate Chat, Inputs, AI models, orchestration, routing, tool and agent operations, Outputs, Artifacts, Projects and other core service functions for the performance of its contract with the User.

The purposes of the processing include, in particular, interpreting the User's instructions, selecting appropriate models and tools, breaking a task into steps and coordinating those steps, carrying out necessary intermediate processing, and generating and providing the result to the User.

If a particular operation is not necessary for performance of the contractual service, Axion does not automatically rely on contractual necessity as the legal basis for that operation.

3.4. File, Document, Research and Execution Functions

If the User uploads a file or document or uses OCR, web search, research, code, Forge, Workflow, sandbox or another execution function, Axion generally processes the data necessary to operate that function for the performance of the requested service.

The purposes of the processing may include, in particular, processing document content, extracting text, locating relevant information on the web or from other external sources, executing code or a workflow, generating technical results and completing the task requested by the User.

Where personal data originates from an external source, Axion uses that data only within the scope of the relevant task and applicable law.

3.5. Connected Services, Integrations and Actions

Processing data from Connected Services and other integrations voluntarily connected by the User is necessary to provide the relevant integration and to perform the task or operation initiated by the User.

Axion processes authorised access, scopes, authorization data and information retrieved or transmitted through the integration only to the extent necessary to operate the relevant function and perform the operation requested by the User.

If performance of an Action requires confirmation or other approval by the User, Axion may process the fact of that approval and related execution data in order to perform the operation securely and in a demonstrable manner. Confirmation does not constitute general consent to processing for other purposes.

3.6. Coin, Payments, Invoicing and Settlement

As a general rule, Axion processes personal data necessary for Coin purchases, Coin balances and usage, and the completion of payments and transactions for the performance of the contract. Online payment transactions are processed by Stripe; Axion may transmit the data necessary to issue invoices to Számlázz.hu.

Processing relating to invoicing, taxation, accounting and other mandatory financial records may be based on compliance with a legal obligation. In accordance with applicable law, billing data may be processed within the Számlázz.hu system and may, where required by law, be made available or disclosed to Axion's accountant, the Hungarian National Tax and Customs Administration (NAV) or another competent authority. Depending on the circumstances, fraud prevention, investigation of transaction abuse and management of legal claims may also be based on Axion's legitimate interests.

3.7. Support and User Enquiries

Depending on the nature of the enquiry, Axion may process personal data necessary to handle support, data protection, technical and other User enquiries on the basis of performance of a contract, compliance with a legal obligation or Axion's legitimate interests.

The purposes of the processing include, in particular, understanding the question or issue, carrying out any necessary technical investigation, responding, troubleshooting, handling complaints and documenting related communications.

3.8. Security, Fraud/Abuse Prevention and Technical Logging

Axion may process personal data to protect the security of the Service, Accounts, infrastructure, Users and third parties, including for authentication and security monitoring, fraud and abuse prevention, detection of unauthorised access and attacks, incident handling, troubleshooting, auditability and system integrity.

As a general rule, such processing may be based on the legitimate interests of Axion and, where applicable, other affected persons, provided that a balancing assessment demonstrates that the processing is necessary and proportionate and that the data subject's rights and freedoms do not override those interests.

Where processing particular security data is necessary to comply with a legal obligation, compliance with that legal obligation may constitute the appropriate legal basis.

3.9. Legal Claims, Authority Requests and Legal Obligations

Axion may process personal data in order to comply with applicable laws and binding obligations imposed by competent authorities or courts, and to establish, exercise or defend legal claims.

Where required by a mandatory legal provision or a properly binding request from a competent authority, processing may be based on compliance with a legal obligation. Depending on the circumstances, documenting legal claims, managing disputes and protecting Axion's rights may also be based on legitimate interests.

In such cases, Axion also seeks to limit the processing and disclosure of data to what is necessary for the relevant legal purpose.

3.10. Analytics and Measurement of Service Use

Axion may use analytics and measurement data to understand use of the Service, measure performance, identify errors and usage patterns, and improve the operation of the product.

The applicable legal basis depends on the technology used and the nature of the processing. Where use of a particular analytics technology or cookie requires consent, Axion uses it only on the basis of appropriate consent. Other appropriately limited and necessary measurement operations may be based on legitimate interests where the conditions of applicable law are satisfied.

3.11. Service Improvement

Axion may process appropriately limited personal data to improve the reliability, usability, performance and functionality of the Service where an appropriate legal basis is available.

Where processing is based on legitimate interests, Axion considers in particular the nature of the data, the data subject's reasonable expectations, the necessity of the processing, potential impacts and the safeguards applied.

Axion does not treat the general purpose of service improvement as unlimited authorisation for any further use of User Content. Where a development purpose requires another legal basis, separate information or consent, that requirement must be satisfied separately.

3.12. Marketing Communications

Axion sends marketing or promotional communications only in accordance with applicable electronic communications, direct marketing and data protection rules.

Depending on the channel and circumstances, the legal basis for marketing communications may be consent or another lawfully available legal basis. Where consent is required, providing consent is voluntary and it may be withdrawn at any time.

Service communications necessary for operation of the Service, Account security, a transaction, legal changes or another non-marketing purpose are not automatically considered marketing communications.

3.13. Consent and Legitimate Interests

Where processing is based on consent, Axion requests consent for the specific purpose and provides appropriate information. Refusal or withdrawal of consent does not affect the lawfulness of processing carried out on the basis of consent before its withdrawal.

Reviewing or accepting the Terms of Service, Privacy Policy or another general legal document does not, in itself, constitute general GDPR consent for all processing purposes.

Where Axion relies on legitimate interests, before or as part of the processing it assesses the existence of the legitimate interest, the necessity of the processing, the impact on the data subject and the balance between the relevant interests, rights and freedoms. The data subject may have a right to object to such processing under the GDPR.

3.14. Special Situations and Changes to the Legal Basis

Additional legal-basis or data-protection requirements apply to processing involving special categories of personal data, children's data, personal data relating to criminal convictions and offences, User Content concerning other persons, and processing carried out through User-operated applications. Detailed rules are set out in particular in Sections 12 and 13.

Axion does not change the legal basis of a processing activity merely by amending this Privacy Policy. If the purpose, circumstances or legal basis of processing materially changes, Axion assesses the lawfulness of the new processing before it begins, provides appropriate new information where necessary and, where required, obtains new consent or establishes another appropriate legal basis.

Identifying a legal basis in this Privacy Policy does not make processing lawful where the conditions for relying on that legal basis are not actually satisfied.

4. Recipients, Processors and Technology Providers

4.1. General Principles

Axion may use external technology providers, infrastructure providers and other recipients in order to operate the Service.

Personal data may be disclosed to or made accessible by such a provider only where this is necessary to operate the relevant Axion function, perform a task requested by the User, pursue a security or operational purpose, comply with a legal obligation, or achieve another lawful processing purpose specified in this Privacy Policy.

Axion does not automatically disclose all personal data to all technology providers.

The providers participating in a particular task may depend, in particular, on the function used by the User, the nature of the Input and the task, Axion's orchestration and routing process, the technical capabilities required and the services available at the relevant time.

Where required by applicable data protection law, Axion applies data processing terms compliant with Article 28 GDPR to the relevant processor.

4.2. Distinction between Processors and Independent Controllers

The data protection role of an external provider is determined by the actual circumstances of the relevant processing operation.

A provider may act as a processor where it processes personal data on Axion's behalf and on Axion's documented instructions. In other situations, a provider may act as an independent controller in respect of processing purposes and essential means that it determines itself.

The fact that a provider is technically involved in delivering an Axion function does not, by itself, determine its GDPR role. The applicable contractual terms, the provider's actual activities and the purposes and means of the relevant processing must also be considered.

Accordingly, the same provider may have different data protection roles in relation to different processing operations.

4.3. Infrastructure and Hosting Providers

Axion may use cloud, hosting, database, storage, networking and related infrastructure providers to operate the Service.

Such providers may process personal data stored or transmitted through Axion's infrastructure to the extent necessary to provide the relevant infrastructure service, maintain availability and security, perform backups and recovery, or provide related technical functionality.

Axion's primary production infrastructure and database may be provided through Microsoft Azure and Azure PostgreSQL services. Further rules concerning processing locations, data residency and international transfers are set out in Section 5.

4.4. Artificial Intelligence and Model Providers

Axion may use external artificial intelligence model providers to interpret Inputs, generate Outputs, perform analysis, support research, process documents, generate or modify code, or perform other AI-supported operations.

Depending on the task and routing decision, relevant Input, context, instructions, files or extracted content, intermediate results and other data necessary for the operation may be transmitted to the AI provider selected for the relevant task.

Axion does not automatically send the entirety of a User's content to every available AI provider. The actual data flow depends on the requested function, orchestration and routing, the selected model or provider, and the technical steps required to perform the task.

AI providers used by Axion may include OpenAI, Anthropic and Google in connection with their respective supported AI services. Provider-specific technical and contractual conditions may change over time.

4.5. Search, Document Processing, Sandbox, Media and Other Technical Providers

Axion may use specialised external providers where a requested function requires web search, information retrieval, OCR or document processing, sandbox or code execution, media or file processing, or another technical capability.

In such cases, the data necessary to perform the relevant operation may be transmitted to or processed through the provider involved in that operation.

Depending on the function, such providers may include Brave for web search, Google for supported document-processing/OCR functionality, E2B for sandbox and code execution, and Cloudinary for supported media and file handling.

The involvement of a provider in one function does not mean that the provider receives data relating to unrelated Axion functions.

4.6. Analytics, Payment, Invoicing and Other Operational Providers

Axion may use external providers for analytics, payment processing, invoicing and other operational functions.

PostHog may be used for web and product analytics subject to the configuration, consent and other requirements described in this Privacy Policy and the applicable Cookie Notice.

Stripe processes online payments and related transaction services. Axion does not store full payment-card numbers, CVC/CVV codes or other complete payment-card authentication data, as described in Section 2.7.

Számlázz.hu / KBOSS.hu Kft. may be used for invoice issuance and related invoicing services. Billing and invoice data may also be subject to statutory accounting and tax requirements.

Depending on the relevant processing operation, these providers may act as processors, independent controllers or in another role recognised by applicable law and contractual arrangements.

4.7. Routing and Data Minimisation

Axion selects providers relevant to the performance of the particular task and structures routing so that the data set necessary and relevant to performance of the task is sent to the relevant provider. The data flow may depend on the function, model, tool or integration used and on the User's instructions.

Data minimisation does not mean that personal data can never be processed by more than one provider in the course of a complex task. Where participation by multiple providers is necessary to perform the requested task, the data may be processed by multiple providers within the scope of the necessary operations.

4.8. Changes to Providers and Current Provider List

Axion's technology providers, models and infrastructure components may change over time. Naming a provider or model in this Privacy Policy does not mean that the relevant provider or model participates in every Axion function or will remain part of the Service indefinitely.

At the time this Privacy Policy was prepared, the principal technology providers used by Axion or planned for use in the production Service include:

Microsoft - Azure hosting, infrastructure and PostgreSQL; OpenAI - AI models and API; Anthropic - Claude AI models and API; Google - Gemini AI service; Google - OAuth/authentication and supported Google integrations; Google - document processing/OCR; Brave - web search; E2B - sandbox and code execution; Cloudinary - media and supported file handling; PostHog - web and product analytics; Stripe - online payments, payment processing and related transaction services; Számlázz.hu / KBOSS.hu Kft. - invoice issuance and related invoicing services.

If there is a material change to the provider set, Axion updates this Privacy Policy or the applicable provider/subprocessor list as appropriate. Section 5 applies to processing locations, transfers outside the EEA and applicable transfer safeguards.

4.9. Axion as Processor and Subprocessors

Where Axion acts as a processor on behalf of a User, an external provider engaged by Axion for the relevant processing may participate in that processing as a subprocessor.

This role may arise in particular in relation to an infrastructure provider or an AI, document-processing, sandbox or other technology provider that actually participates in the relevant User-operated processing.

Detailed rules governing the engagement and replacement of subprocessors, applicable contractual requirements and the rights of the User as controller are set out in Section 13 and, where applicable, the Data Processing Agreement / Data Processing Terms.

5. International Data Transfers

5.1. General Principles

Axion provides services to European users while using international technology providers to operate the Service. As a result, certain personal data may be processed in countries outside the European Economic Area (“EEA”) or may become accessible to providers operating in such countries.

Processing outside the EEA does not in itself mean that a transfer is unlawful. Where an international transfer within the meaning of Chapter V GDPR takes place, Axion applies an appropriate legal basis, transfer mechanism and, where necessary, additional safeguards for the relevant transfer.

5.2. Circumstances Involving Processing Outside the EEA

International data flows may occur, in particular, where an AI, infrastructure, search, document-processing, sandbox, media, analytics or other technology provider used by Axion, or its subprocessor, processes data outside the EEA or provides access from outside the EEA.

The actual processing location may depend on the relevant provider, product, contracting entity, selected region, technical configuration and applicable subprocessor chain.

Not every Axion function and not all User data involves an international transfer; the data flow depends on the service and processing operation actually used.

5.3. Adequacy Decisions and Appropriate Safeguards

Where the European Commission has adopted an adequacy decision covering the relevant third country, territory, sector or appropriate organisational framework, the transfer may take place on the basis of the applicable adequacy framework.

Where no applicable adequacy decision is available, Axion may use appropriate safeguards under Article 46 GDPR, including the European Commission's Standard Contractual Clauses (“SCCs”), where their conditions are satisfied.

Where applicable law or the circumstances of the relevant transfer so require, Axion or the relevant provider may apply additional contractual, technical or organisational measures.

The nature of such measures may depend on the relevant processing and is not necessarily identical for every international data flow.

5.4. EU–U.S. Data Privacy Framework and Standard Contractual Clauses

Where a data importer in the United States validly participates in the EU–U.S. Data Privacy Framework (“EU–U.S. DPF”) and the relevant transfer falls within the scope of its certification, the transfer may, where appropriate, take place on the basis of the European Commission's applicable adequacy decision.

Axion does not automatically assume that an entire U.S. provider or all services of that provider are covered by the EU–U.S. DPF merely because an affiliate or legal entity of the provider participates in the framework. Applicability must be assessed by reference to the actual data importer, its current certification status and the relevant processing.

Where the EU–U.S. DPF is not applicable to a particular transfer, Axion may use another appropriate transfer mechanism, including SCCs.

Where SCCs are used, the applicable module must reflect the actual data protection roles of the parties involved in the transfer. Depending on the circumstances, this may include Controller-to-Controller, Controller-to-Processor or Processor-to-Processor arrangements.

Axion does not rely on the derogations under Article 49 GDPR as a routine general mechanism for regular service-related transfers where an appropriate stable transfer mechanism is required.

5.5. Technology Providers and Processing Locations

The processing locations and international transfer arrangements of the technology providers identified in Section 4 may differ by provider and product and may change over time.

Axion therefore manages the compliance of material international data flows and applicable transfer safeguards actually used in the production Service by reference to the relevant provider and technical configuration.

5.6. Subprocessors and Onward Transfers

Axion's technology providers may engage additional subprocessors or infrastructure providers in order to provide the relevant service. Personal data may therefore be transferred onward from the original recipient to another provider (“onward transfer”).

Axion seeks to ensure that appropriate data protection obligations apply throughout the processor chain it uses and, where an international transfer occurs, that appropriate transfer mechanisms under the GDPR are in place.

The possibility of an onward transfer does not mean that all data is transmitted to every subprocessor; the actual data flow depends on the technical operation of the relevant service and processing.

5.7. Axion as Processor

Where Axion acts as a processor on behalf of a User and the relevant processing involves a transfer outside the EEA or the engagement of a subprocessor, Axion must also ensure an appropriate contractual and transfer framework within the processor chain in accordance with applicable GDPR requirements.

In such a case, the User may be the controller, Axion the processor, and the technology provider engaged by Axion a subprocessor in respect of the relevant processing.

Detailed obligations relating to international transfers and subprocessors for such processing are set out in Section 13 and, where applicable, the Data Processing Agreement / Data Processing Terms.

5.8. Changes, Transparency and Further Information

The legal and technical environment for international transfers, provider chains and available transfer mechanisms may change over time.

If a transfer mechanism previously relied upon ceases to be valid, no longer applies to the relevant data flow or otherwise no longer provides appropriate protection, Axion applies an appropriate alternative mechanism or additional safeguard or, where necessary, modifies, restricts or terminates the relevant data flow.

A data subject may request further information from Axion regarding international transfers concerning that person and the appropriate safeguards applied by contacting support@axionaiapp.com. Where provided by applicable law, the data subject may request appropriate information about, or a copy of, the safeguards used, subject to appropriate protection of trade secrets and the rights of other persons.

6. Retention and Deletion of Personal Data

6.1. General Retention Principles

Axion generally retains personal data only for as long as necessary to fulfil the relevant processing purpose, provide the Service, comply with a legal obligation, pursue a security purpose or establish, exercise or defend a legal claim.

When determining retention periods, Axion takes into account, in particular, the nature of the data, the purpose and legal basis of the processing, deletion actions performed by the User, applicable legal obligations, and the operation of technical systems and external providers.

Deletion does not in every case mean the immediate and simultaneous physical removal of data from all active systems, backups and external provider environments. Axion carries out deletion processes in accordance with the rules set out in this Section.

6.2. Account and Service Data

As a general rule, Axion processes Account, profile, authentication, settings and service data necessary for operation of an active Account for as long as the Account remains active or for as long as necessary to provide the relevant function.

Certain contractual, transactional, security, audit or legal data may be retained after termination of the Account where this is necessary to comply with an applicable legal obligation, establish, exercise or defend a legal claim, prevent fraud or abuse, handle a security incident, or on another appropriate legal basis.

Such exceptional retention does not mean that Axion retains the entire contents of a deleted Account indefinitely.

6.3. Deletion of Chats, Projects, Artifacts, Files and Other User Content

Where the User deletes content in Axion for which the Service provides a deletion function, Axion initiates the deletion process in accordance with the User's request.

A deleted Chat, Project, Artifact, file or other related User Content may first be removed from the active User environment and is then permanently removed from the relevant backend and storage systems in accordance with the technical deletion process.

In the current Axion system, the targeted maximum duration of such a deletion process is 30 days, unless continued retention is justified by an applicable legal obligation, legal claim, security reason or another exception specified in this Privacy Policy.

6.4. Account Deletion and the Maximum 30-Day Deletion Process

When an Account is deleted, Axion initiates the deletion or anonymisation of the Account and related personal data that is not required to be retained further.

Under the current system design, the deletion process associated with Account deletion is completed within a maximum of 30 days in Axion's active systems and data stores falling within the scope of the deletion process, taking into account the technically necessary processing time.

The 30-day period does not override cases in which Axion is legally required to retain certain data for longer, or may retain data for as long as necessary on an appropriate legal basis in connection with a legal claim, security incident, fraud/abuse investigation or another exceptional purpose.

6.5. Backups and Residual Technical Data

Following deletion from the active system, personal data may continue to exist for a limited period in backups, disaster-recovery systems or other technical copies.

The purpose of such backup data is to ensure system recoverability and operational resilience. Personal data remaining in backups after it has already been deleted from active systems is not used by Axion for a new, independent processing purpose; such data may remain only for as long as necessary for the backup and disaster-recovery function and is then deleted or overwritten in accordance with the backup lifecycle.

If previously deleted personal data technically reappears as a result of restoration from a backup, Axion re-applies the previous deletion state through an appropriate procedure, unless an appropriate legal basis exists for continued retention of the data.

6.6. Legal, Financial, Security and Legal-Claims Exceptions

Axion may be required or permitted to retain certain personal data even after deletion initiated by the User or termination of the Account.

This may include, in particular, accounting, tax and invoicing records; evidence of acceptance of contracts and legal documents; data required to comply with obligations imposed by authorities or courts; information necessary to establish, exercise or defend legal claims; and data necessary for the appropriate investigation and documentation of security, fraud or abuse events. Accordingly, invoices and mandatory accounting or tax data processed in the Számlázz.hu system do not automatically fall within Axion's general maximum 30-day deletion process.

Axion retains such data only to the extent and for the period necessary for the relevant exceptional purpose and does not continue to process it for the original service purpose once that purpose has ended, unless a separate appropriate legal basis exists.

6.7. External Providers and Provider-Side Retention

Where personal data is transferred to a technology provider used by Axion, deletion and retention may also depend in part on that provider's technical and contractual data-processing mechanisms.

Accordingly, deletion performed within Axion's own systems does not in every case mean that the data physically disappears at the same moment from every external provider system, temporary store, backup or log.

Axion seeks to use provider and contractual arrangements that provide appropriate deletion and retention rules and, where Axion has the ability or obligation to do so, initiates or enforces the necessary provider-side deletion processes.

Provider-specific retention periods may depend on the provider, product, configuration, relevant data flow and applicable legal obligations. This may be particularly relevant to Stripe's payment/transaction processing and the invoicing, accounting and tax records maintained through Számlázz.hu.

6.8. Axion as Processor

Where Axion acts as a processor on behalf of a User, retention and deletion of personal data processed in the context of User-operated processing are governed primarily by the documented instructions of the User acting as controller, the applicable Data Processing Agreement / Data Processing Terms and the GDPR rules applicable to processors.

Axion deletes or returns such data in accordance with the applicable data-processing terms, unless Union or Member State law requires continued retention of the data.

Data processed by Axion for its own separate purposes as controller—for example for Account administration, billing, security or legal-compliance purposes—remains subject to Axion's retention rules applicable in its capacity as controller.

7. Data Subject Rights and Handling of Requests

7.1. General Rules

Data subjects may have the rights described in this Section under applicable data protection law, in particular the GDPR. The exercise of these rights depends on the circumstances of the relevant processing and the conditions set out in the GDPR.

A data subject may submit a request to Axion, in particular, by e-mail to support@axionaiapp.com. Axion handles the request without undue delay and, as a general rule, within one month of receipt. In the cases provided for by the GDPR, this period may be extended by a further two months; in such a case, Axion informs the data subject of the extension and the reasons for it within the initial one-month period.

As a general rule, requests are handled free of charge. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, Axion may charge a reasonable fee or refuse to act on the request in the manner and subject to the conditions permitted by the GDPR.

If Axion has reasonable doubts concerning the identity of the person making the request, it may request only such additional information as is necessary to confirm that person's identity. Axion does not automatically require submission of an identity document for every data subject request.

7.2. Right of Access

The data subject has the right to obtain confirmation as to whether Axion processes personal data concerning them and, where that is the case, to obtain access to the personal data and the related information required under the GDPR.

The right of access may extend to Account, Chat, Input, Output, Artifact, Project, Connected Service, support, technical or other personal data processed in Axion, provided that the relevant information constitutes personal data concerning the data subject and Axion processes it in its capacity as controller.

When providing a copy, Axion takes into account the rights and freedoms of other persons, as well as secrets protected by applicable law and relevant security interests.

7.3. Right to Rectification

The data subject may request rectification of inaccurate personal data concerning them and, taking into account the purposes of the processing, completion of incomplete personal data.

Where the User can modify the relevant data directly through an appropriate Axion interface, Axion may also draw attention to that option, but this does not remove the data subject's rights under the GDPR where the applicable conditions are satisfied.

7.4. Right to Erasure

The data subject may request erasure of personal data concerning them in the circumstances specified by the GDPR. The right to erasure is not absolute; Axion may refuse or limit erasure where continued processing is necessary, for example, for compliance with a legal obligation, the establishment, exercise or defence of legal claims, or another exception provided for by the GDPR.

Deletion of an Account, Chat, Project, Artifact, file or other content through the Axion interface may, as a product function, initiate the related technical deletion process. Independently of this, the data subject may also submit a separate erasure request under the GDPR.

An erasure request under the GDPR does not necessarily require deletion of the entire Account where the request concerns only specified data or processing. The technical and retention rules governing deletion are described in Section 6.

7.5. Right to Restriction of Processing

The data subject may request restriction of the processing of their personal data in the circumstances specified by the GDPR, for example where the accuracy of the data is contested, the processing is unlawful but the data subject opposes erasure, Axion no longer needs the data but the data subject requires it for a legal claim, or the data subject has objected to the processing and the balancing of interests is still pending.

Where processing is restricted, Axion processes the data further, other than for storage, only under the conditions permitted by the GDPR.

7.6. Right to Data Portability

Where the conditions of the GDPR are satisfied, the data subject has the right to receive personal data concerning them that they have provided to Axion in a structured, commonly used and machine-readable format, and may have the right to transmit those data to another controller.

Data portability may apply in particular to processing based on consent or contract and carried out by automated means. The right does not automatically require Axion to export all of its internal technical data, inferences, system information or data affecting the rights of another person.

7.7. Right to Object

The data subject may, on grounds relating to their particular situation, object to processing based on Article 6(1)(e) or (f) GDPR. In such a case, Axion no longer processes the personal data unless it demonstrates compelling legitimate grounds for the processing that override the interests, rights and freedoms of the data subject, or the processing is related to the establishment, exercise or defence of legal claims.

Where personal data is processed for direct marketing purposes, the data subject may object at any time to processing for such purposes; following such an objection, the personal data will no longer be processed for direct marketing purposes.

7.8. Withdrawal of Consent

Where processing is based on consent, the data subject may withdraw that consent at any time. Withdrawal does not affect the lawfulness of processing based on consent before its withdrawal.

Acceptance or review of the Terms of Service, this Privacy Policy or another general legal document does not, in itself, constitute general consent to the processing of personal data.

7.9. Automated Decision-Making and AI

Axion uses AI models, orchestration, routing and automated technical processes to operate the Service and create Outputs requested by the User.

An AI-generated Output, model selection, routing decision or other automated technical operation does not, by itself, necessarily constitute a decision based solely on automated processing within the meaning of Article 22 GDPR that produces legal effects concerning the data subject or similarly significantly affects them.

If Axion were to introduce processing to which Article 22 GDPR applies, Axion will provide the information and safeguards required by applicable law, including, where relevant, the possibility to request human intervention, express the data subject's point of view and contest the decision.

7.10. Recipients, Processors and Processor Situations

Where Axion fulfils a request for rectification, erasure or restriction, it informs the recipients to whom the relevant personal data has been disclosed where required by the GDPR, unless this proves impossible or involves disproportionate effort. At the data subject's request, Axion may provide information about such recipients within the framework of the GDPR.

Technical fulfilment of a data subject request may require the involvement of Axion's processors or other technology providers.

Where Axion acts solely as processor in respect of particular User-operated processing, the primary recipient of a data subject request is the User acting as controller. Axion assists the controller in fulfilling the request in accordance with the GDPR, documented instructions and the applicable Data Processing Agreement / Data Processing Terms.

7.11. Rights of Other Persons, Representation and Minor Data Subjects

Where a document, Input, Connected Service data, User-operated application or other content processed in Axion contains personal data relating to a third party, the rights of the relevant data subject may be exercised according to the data protection roles applicable to that processing.

A data subject may also act through a representative holding appropriate authorisation. Axion may request information necessary to verify the representative's authority.

The age requirement applicable to use of the Axion Service does not exclude the possibility that content processed by a User may contain personal data relating to a minor. In such a case, data subject rights and any question of representation must be handled in accordance with applicable data protection rules.

7.12. Complaints and Judicial Remedies

The data subject has the right to lodge a complaint with the competent data protection supervisory authority, in particular in the Member State of their habitual residence, place of work or place of the alleged infringement, if they consider that the processing of their personal data infringes the GDPR.

The data subject is also entitled to seek a judicial remedy subject to the conditions set out in the GDPR and other applicable law.

Before lodging a complaint, the data subject may also contact Axion at support@axionaiapp.com so that Axion can investigate and, where possible, resolve the data protection concern. This does not restrict the data subject's right to seek a remedy before a supervisory authority or court.

7.13. Documentation and Technical Fulfilment of Requests

Axion may appropriately document the receipt, handling and fulfilment of data subject requests for the purposes of GDPR compliance, security, auditability and the management of legal claims.

When fulfilling requests, Axion applies appropriate technical and organisational measures to ensure that personal data is not disclosed to an unauthorised person and that fulfilment of the request does not jeopardise the rights of other data subjects or the security of the Service.

Axion's internal product, backend or provider processes may not restrict the exercise of rights to which a data subject is actually entitled under the GDPR. Axion adapts the method of technical implementation to the relevant request and system.

8. Google Services, OAuth and Connected Google Services

8.1. Different Roles of Google Services

Axion may use several distinct Google services. Sign-in with a Google Account, the Google Gemini AI service, document-processing/OCR functions, and Google services separately connected by the User constitute different processing operations.

Signing in with a Google Account does not, by itself, give Axion access to the contents of the User's Gmail, Google Drive, Google Calendar or any other Connected Google Service.

Axion accesses data from such a service only if the User separately connects the relevant integration, authorises the required permissions, and the relevant function or User request actually requires such access.

8.2. Google Login and OAuth Authentication

If the User signs in to Axion using a Google Account, Axion may receive from Google the data necessary for authentication and Account identification, such as the User's name, e-mail address, profile information, provider identifier and related authentication metadata, depending on the applicable OAuth configuration.

The purpose of Google Login is to provide authentication and Account access. Permission granted for authentication must not automatically be interpreted as permission to access the contents of other Google services.

Axion processes authentication data in accordance with the processing and retention rules set out in Sections 2, 3 and 6.

8.3. Connected Google Services and Separate Authorization

Connecting Gmail, Google Drive, Google Calendar or another supported Google service to Axion may require a separate authorization process.

Axion limits the access it requests to the OAuth scopes necessary for operation of the relevant integration. If a function used later requires additional permissions, Axion may request additional or incremental authorization from the User.

The User may decide not to grant the requested access. In that case, the relevant Connected Google Service function may be unavailable or may operate only to a limited extent, while other Axion functions that do not require that access may remain available.

8.4. Data Accessible through Connected Google Services

The categories of Google data accessible to Axion depend on the Connected Google Service, the scopes authorised by the User, the relevant Google API and the task initiated by the User.

In the case of a Gmail integration, Axion may, within the scope of the required permissions, access e-mail messages, message content, senders, recipients, subject lines, attachments and related metadata to perform the task requested by the User.

In the case of a Google Drive integration, Axion may, within the scope of the required permissions, access files, documents, file names, content and related metadata to perform the task requested by the User.

In the case of a Google Calendar integration, Axion may, within the scope of the required permissions, access calendar events, dates and times, participants, descriptions and other related event data and, where supported, may perform calendar operations.

Axion does not assume that the entire contents of a Connected Google Service are necessary for a task; processing is aligned with the authorised scopes and the User's actual request.

8.5. Google Actions and Confirmation

Retrieving or analysing Google data and carrying out a Google operation that has an external effect may constitute different operations.

If Axion performs a supported Action that, for example, sends an e-mail, creates or modifies a calendar event, performs a file operation or causes another external change, the Service may require confirmation or another form of User approval depending on the nature of the operation.

Confirmation applies to execution of the relevant operation and does not constitute general consent to processing Google data for other purposes.

8.6. Google API User Data and Limited Use

Axion uses User data received through Google APIs only to provide authorised functions, perform tasks requested by the User, pursue necessary security and operational purposes, and comply with applicable legal obligations.

When processing Google API User Data, Axion applies the Google API Services User Data Policy and Limited Use requirements applicable to Axion where those requirements apply to the relevant service, scope and processing operation.

Axion does not sell Google API User Data obtained through Google APIs, does not use such data for advertising or retargeting purposes, and does not disclose such data to data brokers.

Axion does not use data received through Google APIs for a purpose that is incompatible with the function authorised by the User or with applicable Google API requirements.

8.7. Google API Data and AI Processing

If the User initiates an Axion task whose performance requires AI processing of data originating from a Connected Google Service, Axion may transmit the data necessary to perform the task to the appropriate AI provider actually participating in the orchestration process.

Such processing may be necessary, for example, where the User requests a summary of an e-mail, analysis of a document, interpretation of calendar information or another AI task based on Google data.

Where necessary to perform the function requested by the User, relevant Google API User Data from the Connected Service may be transmitted to an AI or other technology provider selected by Axion for the relevant task. Axion limits such transmission to the data necessary and relevant to performance of the task. Sections 4 and 5 apply to AI providers, provider routing and international data transfers.

8.8. Tokens, Security, Revocation and Disconnection

Axion may process access tokens, refresh tokens or other authorization data necessary to operate Connected Google Services. Axion treats such data as security-sensitive authentication credentials and protects it through appropriate technical and organisational measures.

The User may revoke access or disconnect the integration through functionality provided by Axion or through the relevant Google Account and security settings, depending on the technical capabilities of the service.

Revocation or disconnection primarily prevents future access. Data previously retrieved from a Connected Google Service and stored in Axion may remain subject to Axion's applicable retention and deletion rules until it is deleted in accordance with the relevant mechanism or another legal basis requires its retention.

8.9. Human Access to Google API User Data

Access by Axion personnel to Google API User Data is restricted and is not permitted merely because technical access may be possible.

Human access may take place only where it is appropriately justified and permitted under the applicable Google API requirements and data protection rules, for example where the User has provided the required affirmative agreement for the relevant data, where access is necessary for security or abuse investigation, where required by law, or where another applicable permitted ground exists.

Axion applies need-to-know access restrictions and appropriate technical and organisational controls to such access.

8.10. User Control, Google Workspace and Shared Accounts

The User is responsible for connecting to Axion only a Google Account and Google data for which the User has appropriate authority, and for reviewing the authorised scopes during the authorization process.

In the case of Google Workspace or another organisational account, the organisation's administrator may apply additional access, application or API restrictions. These may affect which Google integrations and functions Axion can provide.

If more than one person has access to the same Axion Account, the risk of access to Google data connected to that Account and to Outputs created from such data may increase. Appropriate management of authorised Account users and access rights is therefore particularly important.

8.11. Google API Compliance and Changes

Axion aligns its use of Google APIs and OAuth functionality with applicable Google developer, OAuth, API User Data and other relevant requirements.

Available Google integrations, requested scopes, consent and authorization flows, and verification or other compliance requirements imposed by Google may change over time. Axion may accordingly modify the technical operation of an integration, the permissions it requests or this Privacy Policy.

9. Artificial Intelligence, Orchestration and Automated Processing

9.1. Role of Artificial Intelligence in Axion

Artificial intelligence is a core component of the Axion Service. Axion may use one or more AI models, tools and supporting technical systems to interpret User requests, analyse content, conduct research, process documents, generate or modify code, create Outputs and perform other functions requested by the User.

Axion is not based on the assumption that a single AI model performs every task. The Service may use orchestration and routing mechanisms to select and coordinate different models, tools and providers according to the nature of the task.

As a result, the personal data processed in connection with a particular task and the providers participating in that processing may vary depending on the function used and the User's request.

9.2. Inputs, Context and AI Processing

To perform an AI-supported task, Axion may process the User's Input together with context necessary for the task, including relevant conversation history, files, documents, Connected Service data, retrieved information, tool results, Project or Artifact context and other information made available to the Service.

Such context is used to the extent necessary to interpret the request, maintain task continuity, select appropriate processing steps and generate the requested result.

The fact that information is technically available within an Account, Project or Connected Service does not mean that all such information is automatically included in every AI request.

9.3. Orchestration, Routing and Multiple Providers

Axion may analyse a task and route all or part of it to an AI model, tool or technology provider considered appropriate for the relevant operation.

A complex task may be divided into multiple steps, and different steps may be performed by different models, providers or technical tools. Intermediate results may be used as context for subsequent steps where necessary to complete the task.

Accordingly, personal data may in some cases be processed by more than one provider during the performance of a single User request. Axion limits the data transmitted in such processing to the data necessary and relevant to performance of the relevant operation.

Axion does not automatically broadcast the entirety of User Content to all available AI providers.

9.4. AI Providers

Depending on the relevant task, Axion may use AI services provided by OpenAI, Anthropic and Google, as well as other providers that may be introduced in accordance with this Privacy Policy.

The actual provider used for a task may depend on factors such as model capability, task type, context requirements, tool availability, reliability, technical constraints and the Service's routing logic.

Use of a particular provider does not mean that the provider receives all data associated with the User's Account or other unrelated Axion tasks.

Further information concerning technology providers, their roles and international data transfers is set out in Sections 4 and 5.

9.5. Data Minimisation in AI Processing

Axion limits personal data transmitted to an AI model or provider to the data necessary and relevant to performance of the task.

Where technically and functionally appropriate, Axion may structure prompts, context, tool outputs and other data flows so that a provider receives only the information required for the relevant processing step.

Data minimisation does not constitute an absolute guarantee that, in a complex task, personal data will be processed by only one provider; it means that Axion restricts data flows to the scope necessary for actual task performance and does not automatically broadcast the entirety of User Content to all available AI providers.

9.6. AI Outputs and Personal Data

Outputs generated by AI models may themselves contain personal data, including where the User requests analysis, transformation, extraction, summarisation or generation based on personal data contained in an Input, file, Connected Service or other source.

AI-generated Outputs may also contain inaccurate, incomplete, outdated or incorrectly inferred information about an identified or identifiable person.

The User should therefore review AI-generated content before relying on it in circumstances where accuracy, legality, fairness or the rights of another person may be material.

Where an Output is stored as part of a Chat, Artifact, Project or other Axion content, the applicable retention and deletion rules described in Section 6 apply.

9.7. Model Training and Further Provider Use

The manner in which an external AI provider may retain, use or otherwise process data transmitted through its service depends on the relevant product, contractual terms, technical configuration and applicable provider policies.

Axion does not represent that all AI providers or all products of a provider apply identical retention, training or further-use rules.

Axion configures and contracts for production AI services with the objective of limiting provider-side use of User data in accordance with the applicable service terms and Axion's data-protection requirements.

9.8. Human Review and Access

AI processing does not mean that Axion personnel routinely review User Inputs or Outputs.

Human access to User Content is restricted and may occur only where appropriately justified, for example for support requested by the User, investigation of a security or abuse incident, remediation of a technical error, compliance with a legal obligation or another legitimate operational purpose.

Where Google API User Data is involved, the additional restrictions described in Section 8 also apply.

Axion applies need-to-know access controls and appropriate technical and organisational safeguards to such access.

9.9. Automated Decisions and Article 22 GDPR

Axion's use of AI, model selection, orchestration, routing and automated generation of Outputs does not, by itself, mean that Axion makes a decision based solely on automated processing that produces legal effects concerning a data subject or similarly significantly affects that person within the meaning of Article 22 GDPR.

The Service is primarily designed to assist Users in performing tasks and generating results rather than to make legally binding or similarly significant decisions about individuals on Axion's own behalf.

If Axion introduces processing that falls within Article 22 GDPR, Axion will assess the applicable legal basis and exceptions and provide the information, safeguards and rights required by applicable law.

9.10. Special Categories of Data and High-Risk Contexts

AI functions may technically process special categories of personal data or other sensitive information where such data is included in User Content, Connected Service data or another source used for a task.

The technical capability to process such data does not itself establish a lawful basis for doing so. The party acting as controller for the relevant processing is responsible for ensuring that an appropriate legal basis and, where applicable, an Article 9 GDPR condition or other statutory requirement is satisfied.

Users should exercise particular care when using Axion for tasks involving health data, biometric or genetic data, political opinions, religious or philosophical beliefs, trade-union membership, sex life or sexual orientation, criminal-offence data, children or other vulnerable persons, or decisions that may significantly affect individuals.

Further rules concerning sensitive data and User responsibility are set out in Sections 12 and 13.

9.11. External Sources, Search and Retrieval-Augmented Processing

An AI-supported task may use information obtained through web search, external sources, Connected Services, uploaded documents or other retrieval mechanisms.

Such information may be incorporated into the AI context where necessary to perform the User's request. The fact that information is publicly accessible does not necessarily mean that it is not personal data or that every subsequent use is lawful.

Axion processes retrieved personal data within the scope of the relevant task and applicable law. Users remain responsible for the lawfulness of instructions and downstream uses for which they act as controller.

9.12. Changes to AI Models and Orchestration

AI models, provider capabilities, routing rules and orchestration architecture may change over time as Axion develops the Service.

Axion may replace a model, introduce a new provider, modify routing or change the technical steps used to perform a task, provided that the resulting processing remains subject to applicable data-protection requirements and the transparency rules described in this Privacy Policy.

Where a material change affects the categories of personal data processed, purposes, recipients, international transfers or other information that must be disclosed under applicable law, Axion updates the relevant privacy information accordingly.

10. Security and Technical and Organisational Measures

10.1. General Security Principles

Axion applies technical and organisational measures appropriate to the nature, scope, context and purposes of the processing and to the risks presented to the rights and freedoms of natural persons.

Security measures are designed to support the confidentiality, integrity, availability and resilience of systems and services used to process personal data and to reduce the risk of unauthorised access, alteration, disclosure, loss or destruction.

No internet-based or software system can guarantee absolute security. Axion therefore applies a risk-based security approach and reviews and develops relevant controls as the Service, threat environment and technical architecture evolve.

10.2. Access Control and Authentication

Access to Axion systems and personal data is restricted according to role, operational need and the principle of least privilege.

Axion uses authentication and access-control mechanisms appropriate to the relevant system and function and limits administrative or privileged access to persons for whom such access is necessary.

Internal access to User Content or other personal data is subject to the restrictions described in this Privacy Policy, including the need-to-know principles applicable to staff access.

Authentication credentials, tokens, secrets and other security-sensitive information are handled separately from ordinary User Content where technically appropriate and are protected through controls appropriate to their sensitivity.

10.3. Encryption and Transmission Security

Axion uses appropriate technical measures to protect personal data during transmission and, where appropriate to the relevant system and risk, at rest.

Communication between the User and Axion and between relevant system components or providers may be protected through encrypted transport protocols and other technical safeguards.

The specific encryption, key-management and infrastructure controls may depend on the relevant service component, provider and production configuration.

10.4. Infrastructure, Database and Environment Security

Axion's production infrastructure may use Microsoft Azure and Azure PostgreSQL together with other technology providers described in Section 4.

Axion applies environment separation, configuration controls, access restrictions and other infrastructure safeguards appropriate to the architecture of the Service.

Development, testing, sandbox and production environments may have different technical purposes and controls. Axion seeks to prevent production personal data from being unnecessarily copied into development or testing environments.

Where a sandbox or code-execution environment is used for a User task, the data made available to that environment is limited to what is necessary for the relevant execution to the extent supported by the function and technical architecture.

10.5. Tenant and User Separation

Axion is designed to restrict one User's access to data belonging to another User unless access is intentionally provided through a supported sharing, collaboration or other authorised function.

Logical access controls, identifiers, authorisation checks and application-level restrictions may be used to maintain separation between Accounts, Projects, Artifacts and other User resources.

The effectiveness of such separation also depends on secure implementation and configuration; Axion therefore treats authorisation and cross-user access controls as security-sensitive components of the Service.

10.6. Secrets, Tokens and Connected Services

API keys, OAuth tokens, refresh tokens, credentials and other secrets used in connection with Connected Services, integrations or technical functions are treated as security-sensitive data.

Axion limits access to such secrets and uses appropriate storage, transmission and lifecycle controls according to the relevant integration and infrastructure.

Secrets must not be intentionally exposed in Outputs, logs, analytics events or User interfaces except where disclosure is necessary for a function explicitly requested by and appropriately available to the authorised User.

Additional requirements applicable to Google authorization data are described in Section 8.

10.7. Logging, Monitoring, Backup and Vulnerability Management

Axion applies appropriate logging, monitoring, backup, recovery, error-handling and vulnerability-management processes to support the security, availability and integrity of the Service.

Security and technical logs may be used to identify suspicious activity, investigate incidents, troubleshoot failures, support auditability and maintain system integrity.

Logging is designed so that sensitive content and credentials are not collected unnecessarily. Where logs contain personal data, the processing is subject to the purpose, access and retention limitations described in this Privacy Policy.

Backup and recovery processes are subject to the retention and deletion principles described in Section 6.

10.8. Security of External Providers

Axion's security also depends in part on the security of infrastructure, AI, search, document-processing, sandbox, media, analytics, payment and other external providers used to deliver the Service.

Axion assesses provider security and data-protection arrangements to an extent appropriate to the nature and risk of the relevant service and uses contractual, configuration and technical controls where appropriate.

The use of an external provider does not remove Axion's obligations under applicable data protection law where Axion acts as controller or processor for the relevant processing.

10.9. Staff Confidentiality and Access

Persons authorised to process personal data on behalf of Axion are subject to appropriate confidentiality and access restrictions.

Staff access is limited to purposes appropriately justified by the relevant role or task, such as support, security investigation, technical remediation, legal compliance or another legitimate operational purpose.

Axion may maintain records of privileged or administrative activity where appropriate for security and auditability.

Google API User Data is additionally subject to the human-access restrictions described in Section 8.

10.10. Security Incidents and Personal Data Breaches

Axion maintains processes for identifying, assessing, containing, investigating and remediating security incidents that may affect personal data.

If an incident constitutes a personal data breach under the GDPR, Axion assesses the risks to the rights and freedoms of natural persons and fulfils applicable notification and documentation obligations.

Where required by Article 33 GDPR, Axion notifies the competent supervisory authority without undue delay and, where feasible, not later than 72 hours after becoming aware of the personal data breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Where Article 34 GDPR requires communication of a personal data breach to affected data subjects, Axion provides that communication without undue delay, subject to the exceptions provided by applicable law.

Where Axion acts as processor, it notifies the relevant controller of a personal data breach without undue delay in accordance with Article 33(2) GDPR and the applicable Data Processing Agreement / Data Processing Terms.

10.11. Security Responsibilities of Users

Users also play an important role in maintaining the security of their Accounts and User-operated systems.

Users are responsible for protecting their authentication credentials, using appropriate access controls, avoiding unauthorised sharing of Accounts or secrets, reviewing permissions granted to Connected Services, and configuring User-operated applications and workflows appropriately.

If a User modifies, exports, deploys, shares or operates code, an application, workflow or other Artifact created through Axion, the User is responsible for assessing the security implications of those changes and the environment in which the resulting system is used.

Axion's security measures do not replace security controls that the User must implement in systems for which the User determines the purposes, configuration or operation.

10.12. Security Changes and Verification

Axion may modify its security architecture and technical and organisational measures as the Service, infrastructure, provider set and risk environment evolve.

Such changes do not reduce Axion's obligation to apply a level of security appropriate to the risk under applicable data protection law.

11. Cookies, Analytics and Similar Technologies

11.1. General Principles

Axion may use cookies, local storage, software development kit (“SDK”) functions, pixels, identifiers and other similar technologies in connection with its website and Service.

Through these technologies, Axion or a provider engaged by Axion may store information on the User's device or access information already stored there. Axion applies the applicable data-protection and electronic-communications rules according to the purpose and operation of the relevant technology.

11.2. Strictly Necessary Technologies

Axion may use cookies or similar technologies that are strictly necessary to provide a service expressly requested by the User or to ensure the secure operation of the Service.

These may include, in particular, technologies necessary for authentication and session management, security, fraud or abuse prevention, load balancing, essential User preferences and remembering cookie or privacy preferences.

Where applicable law does not require consent for such technologies, Axion may use them without consent to the extent necessary to operate the Service. They must not be used merely to conceal optional analytics or marketing purposes.

11.3. Analytics and PostHog

Axion may use PostHog for web and product analytics in order to understand how Users use the Service, which functions operate properly, where errors or performance issues occur, and how the User experience may be improved.

Analytics data may include, for example, event and feature-usage data, page or screen interactions, technical device and browser information, timestamps, pseudonymous identifiers and, depending on the configuration, network or Account-related metadata.

Use of optional PostHog or other analytics functions is subject to the applicable consent and data-protection requirements.

11.4. Analytics Data Minimisation and Content Restrictions

Axion's analytics system is not intended to collect the full text of Chats, Inputs, Outputs, documents, Connected Service data or other User Content generally for analytics purposes.

In configuring analytics, Axion seeks to use the event and technical data necessary to improve the Service and to apply appropriate masking, suppression, exclusion or other data-minimisation controls where an analytics function may affect sensitive fields or content.

Credentials, passwords, secrets, authorization tokens and other authentication data must not be used as ordinary analytics content.

11.5. Consent and Consent Gating

Where applicable law requires prior consent for the use of an optional analytics cookie or similar technology, Axion activates that technology only after appropriate consent has been obtained.

Refusing optional analytics must not prevent the User from using functions that do not require such analytics technology.

Where technically applicable, Axion structures consent gating so that optional tracking is not loaded or activated before the required consent is given.

The User must be able to withdraw consent as easily as it was given, subject to the technical implementation and requirements of applicable law.

11.6. Consent Banner and Preference Controls

Where required, Axion may provide a cookie or privacy consent banner and preference controls through which the User can accept, reject or manage optional categories.

The design of the consent mechanism must not treat inactivity, pre-ticked optional categories or other conduct that does not constitute valid consent as consent.

Where separate categories are used, the User may be offered distinct controls for, for example, necessary, analytics and any future marketing technologies.

11.7. IP Addresses, Identifiers and Pseudonymous Analytics

Analytics technologies may process IP addresses, device or browser information, session identifiers, pseudonymous identifiers and other technical metadata depending on the relevant configuration.

Where the analytics purpose can be achieved with less identifying information, Axion may use configuration or technical measures that reduce or avoid unnecessary collection of identifying data.

Pseudonymisation does not automatically mean anonymisation. Data remains personal data where a natural person can still be identified directly or indirectly using reasonably available means.

11.8. Session Replay, Autocapture and Sensitive Interfaces

Analytics providers such as PostHog may offer autocapture or session-replay functions capable of recording more detailed User-interface interactions than ordinary event analytics.

Axion does not treat the technical availability or convenience of such functions as sufficient justification for unrestricted recording of User interactions.

If autocapture is used, Axion applies appropriate configuration to exclude or restrict interfaces, fields and elements that may contain personal, sensitive or otherwise unnecessary content.

Session Replay is used only if its necessity, legal basis or consent requirement, masking and suppression controls, sensitive-route exclusions, access restrictions and retention have been appropriately assessed and configured.

11.9. Retention, Aggregation and Marketing Tracking

Axion aligns the retention period for analytics personal data with the analytics purpose, the configuration of the service used and the retention principles set out in Section 6. Where the relevant purpose can be achieved in that manner, Axion may seek to use aggregated or anonymised statistics that are no longer linked to an identifiable person.

Use of Axion's current product-analytics technologies does not, by itself, mean that Axion uses behavioural advertising or advertising profiling carried out by a third party.

If Axion introduces marketing, advertising, retargeting or another tracking technology materially different from its current product analytics in the future, Axion will subject its use to an appropriate separate legal basis and, where required, consent, and will provide Users with appropriate information.

11.10. Cookie Policy, User Controls and Compliance

This Privacy Policy sets out the general data-protection principles governing Axion's use of cookies and similar technologies. Axion may provide detailed and current information on the technologies actually used in a separate Cookie Policy or Cookie Notice, including, in particular, their name, provider, purpose, category, duration, first-party or third-party status and consent status.

Axion determines how to handle Do Not Track, Global Privacy Control or other privacy-preference signals sent by a browser or device in accordance with applicable law, the actual technical implementation and the requirements applicable to the relevant signal. Axion does not state that any such signal is supported unless it has actually been implemented and verified.

12. Minors, Special Categories of Personal Data and Third-Party Data

12.1. Age Requirement for Use of Axion

Axion is intended for persons who are at least 18 years of age. A person under the age of 18 may not create or use an Axion Account.

If Axion reasonably becomes aware that an Account is being used by a person below the applicable age requirement for the Service, Axion may take appropriate measures, including restricting or terminating access to the Account and reviewing the processing of related data.

The age requirement applies to the User of the Service and does not mean that content processed through Axion may contain only data relating to adults.

12.2. Data Relating to Minors in User Content

An Input provided by the User, an uploaded document, Connected Service data, web-research results, a User-operated application or other content may contain personal data relating to a data subject under the age of 18.

Processing such data does not mean that the minor is themselves an Axion User. However, depending on the circumstances of the processing, personal data relating to children may require enhanced protection and particular data-protection attention.

Where the User is the controller for the relevant processing, the User is responsible for ensuring that they have an appropriate legal basis and authority to process children's data made available to Axion and, where necessary, an appropriate information or consent mechanism.

12.3. Special Categories of Personal Data

As a general rule, use of Axion does not require the provision of special categories of personal data within the meaning of Article 9 GDPR.

However, an Input, document, Connected Service data or other content provided by the User may contain personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic or biometric data, data concerning health, or data concerning a person's sex life or sexual orientation.

If such data forms part of a task requested by the User, it may, within the relevant processing, be subject to AI, document, search, storage or other necessary technical processing in accordance with the data flows described in this Privacy Policy.

12.4. Legal Basis for Special Categories of Data and Criminal-Offence Data

Processing special categories of personal data is lawful only where, in addition to an appropriate legal basis under Article 6 GDPR, an applicable condition under Article 9 GDPR is satisfied. Depending on the circumstances of the relevant processing, this may include, for example, explicit consent or another exception provided by law.

Axion does not automatically treat all special-category personal data provided by a User as being processed on the basis of explicit consent; the appropriate legal basis and Article 9 condition must be determined by reference to the relevant processing role and processing operation.

Personal data relating to criminal convictions and offences does not constitute a special category of personal data under Article 9 GDPR but is subject to the separate rules in Article 10 GDPR. Such data may be processed only within the limits permitted by applicable law.

12.5. Personal Data Relating to Third Parties

Content entered into or processed through Axion may contain personal data relating to natural persons other than the User.

If the User provides Axion with another person's personal data, the User is responsible for ensuring that they have appropriate authority to do so and, where the User acts as controller, an appropriate data-protection legal basis, and for fulfilling the applicable transparency and other controller obligations.

Axion is not able, and is not required, to verify in advance the User's legal basis for processing in relation to every individual User Input or uploaded document.

13. Controller and Processor Roles; User-Operated Processing

13.1. Functional Determination of Data Protection Roles

Axion's data protection role must in each case be determined on the basis of the actual circumstances of the relevant processing operation. Axion may act as controller in relation to certain processing operations and as processor in relation to others.

In determining the role, particular consideration must be given to who determines the purposes and essential means of processing personal data and whether Axion carries out the processing for its own purposes or on the basis of the documented instructions of another controller.

Accordingly, multiple distinct data protection roles may exist in parallel within the same User or business relationship.

13.2. When Axion Acts as Controller

Axion may act as controller, in particular, in relation to processing operations for which it determines the purposes and essential means itself in order to operate its own Service.

This may include, in particular, Account creation and management, authentication, billing and the handling of AEC or other service transactions, security and fraud/abuse prevention, support, compliance with legal and regulatory obligations, and processing necessary for the operation and analytics of Axion's own Service.

For such processing operations, Axion itself is responsible for complying with the applicable obligations of a controller. Depending on the relevant service and contractual arrangement, technology providers engaged for those operations may act as processors, subprocessors or independent controllers in another capacity.

13.3. User-Operated Processing and the User's Role as Controller

Where the User determines the purposes and essential means of processing personal data in a User-operated application, workflow or other processing operation, the User may act as controller in respect of that processing.

Such decisions may include, in particular, determining what personal data the application collects, who the data subjects are, the purposes for which the data is processed, which functions use the data, to whom the data is disclosed, how long it needs to be retained, and which integrations or third-party services selected by the User participate in the processing.

Where the User is the controller, the User is responsible, in particular, for the lawful purpose and legal basis of the processing, providing appropriate information to data subjects, application-level data minimisation, obtaining any necessary consents or satisfying other legal-basis requirements, and ensuring the lawfulness of the processing configuration determined by the User.

13.4. Axion as Processor

Where Axion processes personal data for purposes determined by the User, on behalf of the User and on the basis of the User's documented instructions, Axion may act as processor in respect of that processing.

In such cases, Axion complies with the obligations applicable to it under Article 28 GDPR, including, in particular, processing on documented instructions, appropriate confidentiality and security requirements, appropriate management of subprocessors, and assistance to the controller as required by law.

The fact that Axion provides infrastructure, AI functionality, code generation, orchestration, hosting or another technical tool for the operation of a User-operated application or workflow does not, by itself, make Axion the controller of the relevant User-operated processing.

This distinction does not relieve Axion of its obligations applicable as processor or of its controller obligations in relation to processing carried out by Axion for its own purposes.

13.5. User Modifications and User-Generated Code

The User may modify, extend or integrate an application, workflow or code created or supported by Axion with another system. Such modifications may include, for example, adding a new data field, tracking technology, external SDK, database, API, integration or other processing function.

The data-protection consequences of a modification independently determined or implemented by the User are not automatically attributable to Axion. If the modification introduces a new processing purpose, data type, recipient or technology provider, the controller for the relevant processing must assess its lawfulness.

If Axion continues to process certain personal data of the modified solution on behalf of the User, Axion's processor obligations continue to apply in respect of that processing.

13.6. Documented Instructions, Customer Data and Axion Service Data

When acting as processor, Axion processes Customer Data in accordance with the User's documented instructions, the applicable Data Processing Agreement or Data Processing Terms, and applicable law.

Customer Data may include, in particular, personal data relating to end users, customers, employees or other data subjects of a User-operated application or workflow that Axion processes on behalf of the User.

Separate from Customer Data may be data falling within Axion Service Data that Axion processes for its own purposes, such as Account, billing, security, fraud-prevention, support or necessary operational metadata. Axion may act as controller in respect of such data even where it acts as processor for other processing operations within the same business relationship.

If Axion considers that a documented instruction infringes applicable data protection law, Axion may inform the controller in accordance with applicable law and the relevant DPA and may handle the instruction in the manner permitted or required by law.

13.7. Subprocessors

Where Axion acts as processor, it may engage appropriate subprocessors for the processing of Customer Data in accordance with the applicable Data Processing Agreement or Data Processing Terms.

An infrastructure, AI, sandbox, media, document-processing or other technology provider used by Axion may qualify as a subprocessor when it processes Customer Data on Axion's behalf as part of the processor chain. The provider's role must therefore be determined on the basis of the relevant processing and contractual arrangement.

Microsoft Azure, for example, is an important provider of Axion's infrastructure and may act as a subprocessor where it processes Customer Data as part of Axion's processor service. The same principle applies to other technology providers.

The current set of subprocessors, the related services and, where relevant, processing locations may be kept up to date in a separate Subprocessor List or Register.

13.8. Processor Security, Confidentiality and Incidents

When acting as processor, Axion applies appropriate technical and organisational measures to protect Customer Data and ensures that persons authorised to process personal data are subject to appropriate confidentiality obligations or an appropriate statutory duty of confidentiality.

If Axion, acting as processor, becomes aware of a personal data breach affecting the controller's Customer Data, Axion notifies the relevant controller without undue delay and cooperates in handling the incident in accordance with the applicable DPA and law.

The general principles governing data security and incident management are set out in Section 10.

13.9. Data Subject Rights, DPIA and Compliance Assistance

Where the User is the controller of User-operated processing, the User is primarily responsible for handling data subject requests. Taking into account the nature of the processing and within the scope of the information and technical capabilities available to it, Axion provides appropriate assistance to the controller in fulfilling data subject rights under the GDPR where Axion is required to do so as processor.

In accordance with applicable law and the DPA, Axion may provide appropriate assistance to the controller with obligations relating to data security, personal data breaches, data protection impact assessments and, where necessary, prior consultation with a supervisory authority.

Such assistance does not transfer decisions belonging to the controller to Axion and does not automatically alter the parties' data protection roles.

13.10. International Transfers, Deletion and Return

Where Customer Data is transferred outside the European Economic Area or becomes accessible there as part of Axion's processor services, Axion applies the applicable international-transfer requirements and the appropriate safeguards specified in the DPA. The general rules governing international transfers are set out in Section 5.

Upon termination of the processor service or on an appropriate instruction from the controller, Axion deletes or returns Customer Data in accordance with the DPA and applicable law, unless Union or Member State law requires further retention.

Final removal from backups, redundant systems or technical recovery environments may occur with a controlled delay, provided that until removal the data remains segregated and protected and is not restored to ordinary business processing.

13.11. Data Processing Agreement

This Privacy Policy provides a general explanation for Users of Axion's roles as controller and processor, but does not replace a data processing agreement under Article 28 GDPR.

Where Axion acts as processor in respect of a processing operation, that processing may also be subject to Axion's Data Processing Agreement or Data Processing Terms, which sets out in detail, in particular, the subject matter and duration of the processing, its nature and purpose, the categories of data and data subjects concerned, the controller's instructions, confidentiality and security requirements, subprocessors, assistance with data subject rights and DPIAs, incident handling, deletion or return, and applicable audit and compliance conditions.

The Privacy Policy and the DPA perform different functions; for processing carried out by Axion as processor, the detailed processor obligations are governed primarily by the applicable DPA.

13.12. Mixed Roles, Joint Controllership and Review

Within the same User relationship, Axion may have different data protection roles in relation to different processing operations. The fact that Axion acts as processor for the processing of Customer Data does not mean that it also acts as processor for its own Account, billing, security, support or other processing carried out for independent purposes.

A joint-controller relationship does not arise automatically merely because Axion and the User participate in the same technical system or service chain. If the parties actually determine jointly the purposes and essential means of a specific processing operation, that processing may require a separate assessment under Article 26 GDPR.

Axion may review its controller/processor role assessment, subprocessor compliance and related DPA terms as the Service and processing operations evolve.

14. Final Data Protection Provisions, Transparency and Governance

14.1. Transparency and Availability of the Privacy Policy

Axion provides concise, transparent, intelligible and easily accessible information about the processing of personal data. This Privacy Policy describes the general framework of Axion's principal processing operations, data protection roles, categories of recipients, retention principles and data subject rights.

The Privacy Policy may be made available on Axion's website and, where relevant, through interfaces associated with Account creation, sign-in or use of the Service. Axion may also provide additional layered or contextual privacy notices for particular functions or processing operations.

Reading, acknowledging or—where the applicable process requires it—accepting the Privacy Policy does not, in itself, constitute consent under the GDPR to all processing carried out by Axion. Where a processing operation requires consent, Axion requests it separately in accordance with applicable law.

14.2. Controller and Data Protection Contact

For processing carried out by Axion for its own purposes, the controller is the legal entity operating the Axion Service and identified in this Privacy Policy or on the related legal interfaces.

For data protection, data subject rights or security enquiries, Axion can be contacted at support@axionaiapp.com, including where the data subject does not have an Axion Account or cannot access it.

If Axion becomes legally required to appoint a Data Protection Officer in the future, or voluntarily appoints one, Axion will publish the Data Protection Officer's contact details as required by applicable law.

14.3. Related Legal and Data Protection Documents

This Privacy Policy forms part of Axion's broader legal and data protection documentation. Additional documents may apply to use of the Service and to particular processing operations, including, in particular, the Terms and Conditions or Terms of Service, the Acceptable Use Policy, the Cookie Policy or Cookie Notice, AI transparency information, security/trust information and, where Axion carries out processing as a processor, the Data Processing Agreement or Data Processing Terms.

These documents serve different functions. The Privacy Policy primarily provides information about the processing of personal data and data subject rights; the Terms govern the service relationship; the Cookie Policy describes in detail the use of cookies and similar technologies; and the DPA governs the processing conditions between controller and processor under Article 28 GDPR.

Where a particular function or processing operation requires separate information or terms, Axion may make those available separately at the relevant point.

14.4. Amendments to the Privacy Policy

Axion may amend this Privacy Policy from time to time, in particular as a result of changes to the Service, processing operations, technology providers, applicable laws, supervisory practice, security requirements or compliance processes.

In the event of a material privacy-related change, Axion informs data subjects in an appropriate manner according to applicable law and the significance of the change, for example within the Service, on the website, by e-mail or through another appropriate channel.

An amendment to the Privacy Policy does not, by itself, create a new legal basis for processing where applicable law requires separate consent, a contractual basis, a legitimate-interests assessment or another condition for the relevant legal basis. If new or modified processing requires an additional legal condition, Axion satisfies that requirement separately.

The version of the Privacy Policy currently in force is made available to the User.

14.5. Effective Date, Versions and Language Versions

Axion indicates the effective date and date of last update of this Privacy Policy and, where used, its version number in the document or on the interface through which it is published.

Axion may retain previous versions for legal, compliance or evidentiary purposes and may make them available where appropriate.

The Privacy Policy may be available in multiple languages. Axion determines the rule governing precedence between different language versions consistently with the complete set of Axion legal documentation.

This English version corresponds to version 1.0, effective and last updated on 17 August 2026. In the event of a discrepancy between the Hungarian and English versions, the Hungarian version prevails to the extent permitted by applicable mandatory law.

14.6. Supervisory Authority, Complaints and Judicial Remedies

A data subject is entitled to raise a data protection complaint with Axion and to lodge a complaint with the supervisory authority competent under the applicable GDPR rules, in particular in the Member State of the data subject's habitual residence, place of work or place of the alleged infringement.

In view of Axion's operation as a controller in Hungary, the details of the Hungarian supervisory authority must be accurately included in the final Privacy Policy.

Submitting a complaint or contacting Axion in advance is not a precondition for the data subject to lodge a complaint with a supervisory authority or seek a judicial remedy under applicable law.

More detailed rules concerning data subject rights and remedies are set out in Section 7.

Hungarian supervisory authority: National Authority for Data Protection and Freedom of Information (NAIH), 1055 Budapest, Falk Miksa utca 9-11., Hungary; postal address: 1363 Budapest, Pf. 9.; e-mail: ugyfelszolgalat@naih.hu; website: https://www.naih.hu.

14.7. Privacy Governance and Accountability

Axion maintains appropriate internal privacy governance and accountability processes in order to document the compliance of its processing operations and review them as the Service evolves.

Depending on the nature of the processing and applicable legal requirements, such documentation may include, in particular, records of processing activities (ROPA), processor records, legitimate interests assessments (LIA), data

protection impact assessments (DPIA), vendor and subprocessor reviews, international-transfer assessments, privacy reviews, security and incident documentation and other compliance records.

Detailed internal compliance documentation does not necessarily form part of this public Privacy Policy. Axion may nevertheless be required under the GDPR or other applicable law to make appropriate parts of such documentation available to a supervisory authority or another entitled party.

14.8. Government, Regulatory and Law-Enforcement Requests

Axion cooperates with competent authorities and courts in accordance with applicable law. Axion discloses personal data in response to a regulatory, judicial or other law-enforcement request only where an appropriate legal basis, legal obligation or other applicable legal authorisation exists.

Axion may assess the lawfulness, authority and scope of a request in accordance with applicable law and, where lawful and appropriate, may seek to limit the data disclosed to what is necessary to comply with the request.

Where informing the data subject or controller is not prohibited by law, Axion may provide appropriate information having regard to the circumstances and its legal obligations.

14.9. Succession, Actual Processing and Primacy of Rights

In the event of a reorganisation, succession, merger, acquisition, transfer of assets or a business line, or another corporate transaction involving Axion, personal data may be transferred to the extent necessary and lawful for the transaction, or the identity of the controller may change. In such a case, Axion provides appropriate data protection safeguards and information as required by applicable law.

Axion maintains and updates this Privacy Policy so that it appropriately reflects the processing actually carried out. If a discrepancy between actual processing and the documentation is identified, Axion corrects the processing, the documentation or both in accordance with applicable law.

Nothing in this Privacy Policy may be interpreted as limiting the exercise of any rights available to a data subject under the GDPR or other mandatorily applicable law.

14.10. Final Provisions

If any provision of this Privacy Policy is found to be wholly or partly invalid, unlawful or unenforceable, this does not, to the extent permitted by applicable law, affect the validity of the remaining provisions.

This Privacy Policy must be interpreted together with the actual operation of the Axion Service, applicable law and the related legal documents. In the event of a conflict, mandatory provisions of applicable law prevail.

The final effective date and version number of the Privacy Policy will be stated when the document is published.

Last updated: 17 August 2026
Effective date: 17 August 2026
Version: 1.0