AXION ADATKEZELÉSI TÁJÉKOZTATÓ

1. Bevezetés, adatkezelő és a tájékoztató hatálya

1.1. Az Adatkezelési Tájékoztató célja

Jelen Adatkezelési Tájékoztató („Adatkezelési Tájékoztató”) ismerteti, hogy az Axion szolgáltatás nyújtása során milyen személyes adatok kezelhetők, milyen célból és jogalapon történhet az adatkezelés, kik férhetnek hozzá a személyes adatokhoz, milyen adatfeldolgozók és más címzettek vehetnek részt az adatkezelésben, mennyi ideig őrizhetők meg az adatok, valamint milyen jogok illetik meg az érintetteket.

Az Adatkezelési Tájékoztató célja továbbá, hogy átlátható tájékoztatást nyújtson az Axion mesterséges intelligencián, modell-orchestrationön, külső technológiai szolgáltatókon, integrációkon, kódfuttatási és egyéb technikai környezeteken alapuló működéséhez kapcsolódó személyesadat-kezelésről.

Az Adatkezelési Tájékoztató különösen az Európai Parlament és a Tanács (EU) 2016/679 rendelete („GDPR”), valamint az egyéb alkalmazandó adatvédelmi jogszabályok alapján nyújtandó tájékoztatást tartalmazza.

1.2. Az adatkezelő

Az Axion szolgáltatás működtetője és a jelen Adatkezelési Tájékoztató hatálya alá tartozó adatkezelések tekintetében – az e Tájékoztatóban meghatározott kivételekkel – az adatkezelő:

Leiter Miklós Patrik

Székhely: 4090 Polgár Hunyadi utca 3.

Nyilvántartási szám / egyéni vállalkozói nyilvántartási szám: 62674771

Adószám: 92281868-1-29

E-mail: support@axionaiapp.com

Weboldal: https://axionaiapp.com

(a továbbiakban: „Axion”, „Adatkezelő” vagy „Szolgáltató”).

Az Axion adatkezelőként határozza meg azon személyesadat-kezelések célját és lényeges eszközeit, amelyeket saját szolgáltatásának biztosítása, működtetése, biztonsága, adminisztrációja és fejlesztése érdekében végez.

1.3. Az Adatkezelési Tájékoztató hatálya

Jelen Adatkezelési Tájékoztató az Axion által adatkezelőként végzett személyesadat-kezelésekre vonatkozik.

Ide tartozhat különösen a személyes adatok kezelése:

a) az Axion Account létrehozása és kezelése;

b) a felhasználó azonosítása és hitelesítése;

c) az Axion szolgáltatásainak biztosítása;

d) a Chat és más felhasználói interakciók működtetése;

e) Inputok, Outputok, Artifacts, Projects és más felhasználói tartalmak kezelése;

f) mesterségesintelligencia-modellek és orchestration folyamatok működtetése;

g) fájlok, dokumentumok, képek és más tartalmak feldolgozása;

h) webes keresés, információ-visszakeresés és kapcsolódó funkciók biztosítása;

i) Axion Forge, Workflow, sandbox és más végrehajtási környezetek működtetése;

j) Connected Accounts, Connected Services, integrációk és Actions működtetése;

k) Axion Coin, vásárlások és kapcsolódó elszámolási folyamatok kezelése;

l) support és panaszkezelés;

m) a szolgáltatás biztonságának fenntartása, visszaélések megelőzése és kivizsgálása;

n) technikai, biztonsági és audit naplók kezelése;

o) a szolgáltatás működésének elemzése és – az alkalmazandó szabályok szerint – analitikai funkciók biztosítása; valamint

p) az Axion működtetéséhez kapcsolódó jogi és adminisztratív kötelezettségek teljesítése.

Az egyes adatkezelések részletes célját, jogalapját, az érintett személyes adatok kategóriáit, címzettjeit és megőrzési idejét jelen Adatkezelési Tájékoztató további fejezetei határozzák meg.

1.4. Az Axion mint adatkezelő

Az Axion főszabály szerint adatkezelőként jár el, amikor a személyes adatok kezelésének célját és lényeges eszközeit az Axion szolgáltatás saját működtetésével kapcsolatban maga határozza meg.

Ide tartozhat különösen az Account működtetéséhez, hitelesítéshez, szolgáltatásnyújtáshoz, biztonsághoz, Coin elszámoláshoz, supporthoz, jogi megfeleléshez és az Axion saját működésének adminisztrációjához szükséges adatkezelés.

Az, hogy az Axion egy adott adatkezelési művelet során adatkezelőként jár-e el, nem kizárólag az alkalmazott technológiától vagy az adat tárolási helyétől függ, hanem attól is, hogy az adott adatkezelés célját és lényeges eszközeit ténylegesen ki határozza meg.

1.5. Az Axion mint adatfeldolgozó

Bizonyos esetekben az Axion nem saját adatkezelési céljára, hanem egy Felhasználó nevében és utasításai alapján dolgozhat fel személyes adatokat.

Ez különösen akkor fordulhat elő, ha egy Felhasználó az Axion segítségével létrehozott, módosított, telepített vagy az Axion által biztosított infrastruktúrán működtetett alkalmazás, szoftver, workflow, automatizáció vagy más rendszer útján harmadik személyek személyes adatait kezeli saját céljaira.

Amennyiben a személyes adatok kezelésének célját és lényeges eszközeit a Felhasználó határozza meg, és az Axion a személyes adatokat a Felhasználó nevében és utasításai alapján dolgozza fel, az adott adatkezelés tekintetében főszabály szerint a Felhasználó minősül adatkezelőnek, az Axion pedig adatfeldolgozóként jár el.

Az Axion adatfeldolgozóként végzett adatkezelésére külön adatfeldolgozási feltételek, Data Processing Agreement vagy más, a GDPR 28. cikkének megfelelő szerződéses rendelkezések vonatkozhatnak.

Jelen Adatkezelési Tájékoztató elsősorban az Axion adatkezelőként végzett adatkezeléséről nyújt tájékoztatást, és önmagában nem helyettesíti az Axion adatfeldolgozói tevékenységére alkalmazandó adatfeldolgozási megállapodást.

1.6. Felhasználó által üzemeltetett alkalmazások és rendszerek

Az Axion lehetővé teheti alkalmazások, weboldalak, programkódok, workflow-k, automatizációk, szolgáltatások és más szoftveres rendszerek létrehozását, módosítását, telepítését vagy működtetését.

Az a tény, hogy egy alkalmazást vagy más rendszert részben vagy egészben az Axion segítségével hoztak létre, módosítottak, telepítettek vagy az Axion technikai infrastruktúráján működtetnek, önmagában nem jelenti azt, hogy az Axion az adott alkalmazás által végzett személyesadat-kezelés adatkezelőjévé válik.

Ha a Felhasználó határozza meg, hogy az általa üzemeltetett alkalmazás:

a) milyen személyes adatokat gyűjt vagy kezel;

b) milyen személyektől gyűjt adatokat;

c) milyen célból kezeli azokat;

d) hogyan használja fel az adatokat;

e) kinek továbbítja vagy teszi hozzáférhetővé azokat;

f) mennyi ideig őrzi meg azokat; vagy

g) milyen funkciókat biztosít saját felhasználói számára,

akkor az ebből eredő adatkezelés tekintetében főszabály szerint a Felhasználó felel az alkalmazandó adatvédelmi követelmények teljesítéséért.

Ez magában foglalhatja különösen a megfelelő jogalap biztosítását, az érintettek megfelelő tájékoztatását, az érintetti jogok biztosítását, a szükséges hozzájárulások beszerzését, az adatmegőrzési szabályok meghatározását, a megfelelő hozzáférés-kezelést és biztonsági intézkedéseket, valamint az alkalmazandó adatvédelmi jogszabályoknak való megfelelést.

Amennyiben az Axion infrastruktúrája az ilyen alkalmazás működése során a Felhasználó nevében személyes adatokat dolgoz fel, az Axion az adott feldolgozás tekintetében adatfeldolgozóként járhat el.

Az Axion ilyen adatfeldolgozói szerepe nem teszi az Axiont az alkalmazás által végzett adatkezelés céljainak meghatározójává, és nem ruházza át az Axionra a Felhasználó adatkezelőként fennálló kötelezettségeit.

Az Axion ugyanakkor önálló adatkezelőként járhat el az ilyen alkalmazás működésével összefüggő olyan elkülönült adatkezelések tekintetében, amelyek célját és lényeges eszközeit maga az Axion határozza meg, például saját Account-adminisztrációja, biztonsági naplózása, visszaélés-megelőzése, számlázása vagy jogi kötelezettségeinek teljesítése érdekében.

Az adatkezelői és adatfeldolgozói szerepet ezért minden esetben az adott konkrét adatkezelési művelet alapján kell meghatározni.

1.7. Adatfeldolgozók, technológiai szolgáltatók és harmadik felek

Az Axion működtetéséhez külső technológiai és infrastruktúra-szolgáltatókat vehet igénybe.

E szolgáltatók az adott adatkezelés körülményeitől, a vonatkozó szerződéses feltételektől és az alkalmazandó jogtól függően adatfeldolgozóként, al-adatfeldolgozóként vagy bizonyos elkülönült adatkezelések tekintetében önálló adatkezelőként járhatnak el.

Az Axion által igénybe vett technológiai szolgáltatók közé tartozhatnak különösen mesterségesintelligencia-modellek szolgáltatói, felhő- és adatbázis-infrastruktúra szolgáltatók, keresési szolgáltatók, dokumentumfeldolgozási és OCR szolgáltatók, média- és fájlkezelési szolgáltatók, sandbox és kódfuttatási szolgáltatók, valamint analitikai szolgáltatók.

Az Axion nem feltétlenül továbbít minden személyes adatot minden technológiai szolgáltató részére.

Az Axion által alkalmazott orchestration, routing és technikai folyamatok alapján az adott feladat végrehajtásában csak az ahhoz szükséges szolgáltatók vehetnek részt, és az adott szolgáltató részére csak az adott művelet végrehajtásához szükséges vagy azzal összefüggő adat kerülhet továbbításra vagy válhat hozzáférhetővé, az Axion technikai működésének és az alkalmazandó követelményeknek megfelelően.

Az adatfeldolgozók, címzettek, nemzetközi adattovábbítások és az egyes technológiai szolgáltatók szerepének részletes szabályait jelen Adatkezelési Tájékoztató további fejezetei tartalmazzák.

1.8. Az Axion munkatársainak hozzáférése

A személyes adatokhoz való belső hozzáférés nem korlátlan.

Az Axion személyes adatokhoz hozzáféréssel rendelkező munkatársai kizárólag olyan mértékben férhetnek hozzá személyes adatokhoz, amennyiben az az adott feladat ellátásához megfelelően indokolt és szükséges.

Ilyen hozzáférés különösen support, biztonsági incidens vizsgálata, visszaélés megelőzése vagy kivizsgálása, technikai hiba elhárítása, jogi kötelezettség teljesítése vagy más megfelelően indokolt üzemeltetési cél érdekében történhet.

A technikai lehetőség egy személyes adat elérésére önmagában nem jelenti azt, hogy az Axion munkatársa jogosult az adatot bármilyen célból megtekinteni vagy felhasználni.

Az Axion a belső hozzáféréseket a szolgáltatás méretéhez, működéséhez és kockázataihoz igazodó technikai és szervezési intézkedésekkel korlátozza.

1.9. Harmadik fél által nyújtott szolgáltatások

Az Axion bizonyos funkciói lehetővé tehetik, hogy a Felhasználó harmadik fél által működtetett szolgáltatást, fiókot, alkalmazást vagy rendszert kapcsoljon az Axionhoz.

Az ilyen Connected Service vagy más külső szolgáltatás saját működése során az adott harmadik fél a saját adatkezelési céljai tekintetében önálló adatkezelőként is eljárhat.

A harmadik fél saját szolgáltatásának adatkezelésére annak saját adatvédelmi tájékoztatója és feltételei is vonatkozhatnak.

Az Axion Adatkezelési Tájékoztatója nem szabályozza az olyan harmadik fél által saját céljára végzett adatkezelést, amelynek célját és eszközeit az Axion nem határozza meg.

Amennyiben azonban az Axion egy Connected Service-ből a Felhasználó kérésére adatot kér le, használ fel vagy továbbít az Axion szolgáltatás működtetése érdekében, az Axion által végzett adatkezelésre jelen Adatkezelési Tájékoztató megfelelő rendelkezései alkalmazandók.

1.10. Google-hitelesítés és Connected Google Services

Az Axion lehetővé teheti a Google-fiókon keresztül történő regisztrációt vagy bejelentkezést.

A Google-fiókkal történő hitelesítés nem azonos a Google által biztosított további szolgáltatások – például Gmail, Google Drive, Google Calendar vagy más Google szolgáltatás – Axionhoz történő csatlakoztatásával.

Az Axion a regisztráció és bejelentkezés során csak az Account létrehozásához, azonosításához és hitelesítéséhez szükséges vagy az adott funkcióhoz megfelelő Google-fiókadatokhoz kér hozzáférést.

Ha a Felhasználó később valamely további Google szolgáltatást kapcsol az Axionhoz, az Axion az adott integrációhoz szükséges külön hozzáférési jogosultságokat kérhet.

Az ilyen hozzáférésekre, az alkalmazott jogosultsági körökre (scope), a Google API-kon keresztül elérhető adatok kezelésére, a hozzáférési tokenek kezelésére és a kapcsolat megszüntetésére jelen Adatkezelési Tájékoztató Connected Accounts és integrációk kezelésére vonatkozó rendelkezései alkalmazandók.

1.11. Az Adatkezelési Tájékoztató kapcsolata más Axion dokumentumokkal

Jelen Adatkezelési Tájékoztató az Axion adatvédelmi tájékoztató dokumentuma, és elsősorban a személyes adatok kezeléséről nyújt tájékoztatást.

Az Axion használatának szerződéses feltételeit az Általános Szerződési Feltételek határozzák meg.

Az Axion megengedett és tiltott használatára vonatkozó szabályokat az Acceptable Use Policy tartalmazza, amely az Általános Szerződési Feltételek részét képezi.

A cookie-k, hasonló technológiák és az azokhoz kapcsolódó adatkezelés részletes szabályait a Cookie Tájékoztató tartalmazza.

Az Axion mesterségesintelligencia-rendszereinek működésére, az AI által létrehozott tartalomra és az alkalmazandó átláthatósági információkra vonatkozó további tájékoztatást az AI Transparency Notice tartalmazhatja.

Az Axion biztonsági megközelítésére vonatkozó további információkat a Security & Trust / Security Notice tartalmazhatja.

Amennyiben az Axion valamely Felhasználó nevében adatfeldolgozóként jár el, az ilyen adatfeldolgozásra külön Data Processing Agreement / Data Processing Terms vonatkozhat.

Jelen Adatkezelési Tájékoztató tudomásulvétele vagy megismerése önmagában nem minősül általános adatkezelési hozzájárulásnak.

Az Axion az egyes személyesadat-kezelési műveleteket az adott adatkezeléshez megfelelő, jelen Adatkezelési Tájékoztatóban meghatározott jogalap alapján végzi.

2. A kezelt személyes adatok kategóriái és forrásai

2.1. Általános elvek és adatforrások

Az Axion által kezelt személyes adatok köre attól függ, hogy a Felhasználó mely funkciókat használja, milyen tartalmat ad meg, milyen integrációkat kapcsol össze, és milyen műveleteket végez a szolgáltatásban. Nem minden, e fejezetben felsorolt adatkategória kerül kezelésre minden Felhasználó esetében.

A személyes adatok származhatnak közvetlenül a Felhasználótól; a Felhasználó által feltöltött vagy létrehozott tartalomból; a Felhasználó által összekapcsolt külső szolgáltatásokból; az Axion technikai rendszereiből és infrastruktúrájából; külső vagy nyilvánosan hozzáférhető forrásokból; valamint az AI-, orchestration-, research- vagy más feldolgozási műveletek során létrejövő eredményekből és metaadatokból.

Az Axion a személyes adatok kezelését az adott funkció, feladat, biztonsági vagy jogi cél szempontjából szükséges és releváns adatokra korlátozza.

2.2. Account-, profil- és hitelesítési adatok

Az Axion Account létrehozása, kezelése és a Felhasználó hitelesítése során kezelhetünk különösen nevet vagy megjelenített nevet, e-mail-címet, belső Account- és User-azonosítókat, profilképet vagy avatarra vonatkozó adatot, nyelvi és felhasználói beállításokat, Account státuszt, valamint a regisztrációhoz és jogi dokumentumokhoz kapcsolódó esemény- és verzióadatokat.

Google vagy más támogatott külső hitelesítési szolgáltató használata esetén kezelhetjük a hitelesítéshez szükséges provider-azonosítókat, OAuth- vagy hasonló hitelesítési metaadatokat, valamint a bejelentkezési és munkamenet-biztonsági adatokat.

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

Az Axion használata során a Felhasználó által megadott vagy létrehozott tartalom személyes adatot tartalmazhat. Ide tartozhat különösen a Chat és más Input tartalma, promptok, utasítások, üzenetek, feltöltött fájlok és dokumentumok, azok neve, formátuma, metaadatai és feldolgozott vagy OCR-rel kinyert tartalma.

Személyes adat jelenhet meg az Axion által létrehozott Outputokban, összefoglalókban, elemzésekben, kódban, dokumentumokban és más eredményekben, továbbá az Artifacts és Projects tartalmában, verzióiban, kapcsolódó metaadataiban és provenance-információiban.

Az Axion nem feltételezi, hogy minden Felhasználói tartalom személyes adatot tartalmaz; a tényleges adatkör a Felhasználó által megadott vagy a feladat végrehajtása során létrejövő tartalomtól függ.

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

Az Axion AI- és orchestration-rendszere a feladat teljesítéséhez kapcsolódó személyes adatot tartalmazó technikai vagy tartalmi adatokat is kezelhet. Ide tartozhatnak különösen a feladatleírások, routing- és modellválasztási információk, feladatlépések, tool- vagy agent-műveletek, köztes eredmények, végrehajtási állapotok, hibák és más, a feladat koordinálásához szükséges metaadatok.

Webes keresés, research vagy külső forrás használata esetén az Axion a keresési lekérdezést, a találatokból vagy más forrásból származó releváns információt, forrás- és hivatkozási adatokat, valamint a kutatási eredmény összeállításához szükséges adatokat kezelheti. Külső vagy nyilvános forrásból származó információ természetes személyre vonatkozó személyes adatot is tartalmazhat.

Kód-, Forge-, Workflow-, sandbox- vagy más végrehajtási funkció használatakor kezelhetünk programkódot, konfigurációt, futási inputot és outputot, technikai logokat, hibaüzeneteket, környezeti és végrehajtási metaadatokat.

2.5. Connected Services, integrációk és Actions adatai

Ha a Felhasználó külső szolgáltatást vagy Connected Accountot kapcsol az Axionhoz, kezelhetjük az integráció azonosításához szükséges account- és provider-adatokat, engedélyezett scope-okat és jogosultságokat, tokeneket vagy más authorization adatokat, valamint az adott Felhasználói kérés teljesítéséhez a külső szolgáltatásból lekért vagy oda továbbított adatokat.

Az Axion által kezdeményezett vagy támogatott Actionök esetén kezelhetjük a művelet típusát, célrendszerét, a művelethez szükséges adatokat, a Felhasználó által adott confirmation vagy jóváhagyás tényét és idejét, valamint a végrehajtás állapotát és eredményét.

A Connected Service összekapcsolása nem jelenti azt, hogy az Axion automatikusan hozzáfér a külső account valamennyi adatához. A tényleges hozzáférést az engedélyezett scope, a provider technikai működése és a Felhasználó által kezdeményezett művelet határozza meg.

2.6. Technikai, eszköz-, biztonsági és naplóadatok

Az Axion a szolgáltatás működtetése, biztonsága, hibakeresése, abuse- és fraud-prevention, valamint infrastruktúra-védelem érdekében technikai és naplóadatokat kezelhet.

Ilyen adat lehet különösen az IP-cím, időbélyeg, session- és request-azonosító, böngészőre vagy eszközre vonatkozó technikai információ, hálózati és rendszer-metaadat, endpoint- és műveleti információ, authentication- és security event, hibakód, teljesítményadat, valamint audit- vagy biztonsági naplóbejegyzés.

Az Axion törekszik arra, hogy a technikai naplókba ne kerüljön több Felhasználói tartalom vagy érzékeny adat, mint amennyi az adott technikai vagy biztonsági célhoz szükséges.

2.7. Coin-, vásárlási, számlázási és tranzakciós adatok

Az Axion Coin-rendszerének, vásárlásoknak és kapcsolódó pénzügyi folyamatoknak a működtetése során kezelhetünk különösen Coin-egyenlegre, Coin-vásárlásra és felhasználásra, csomagra vagy termékre, összegre, pénznemre, tranzakciós azonosítóra, státuszra, időpontra, számlázásra és visszatérítésre vonatkozó adatokat.

Az online fizetések feldolgozását Stripe végzi. Az Axion nem tárol teljes bankkártyaszámot, CVC/CVV-kódot vagy más teljes fizetésikártya-hitelesítési adatot. Az Axion a Stripe-tól a tranzakció és a kapcsolódó szolgáltatás kezeléséhez szükséges korlátozott adatokat kaphat, például fizetési státuszt, tranzakció- vagy referenciaazonosítót, összeget, pénznemet, visszatérítésre, chargebackre vagy más kapcsolódó tranzakciós eseményre vonatkozó információt.

A számlakiállításhoz szükséges adatokat az Axion a Számlázz.hu rendszerének továbbíthatja. A kiállított számlák és azok kapcsolódó számlázási nyilvántartása a Számlázz.hu rendszerében kerül kezelésre és megőrzésre az alkalmazandó számviteli, adózási és más jogszabályi követelmények szerint.

2.8. Support-, kommunikációs és analitikai adatok

Ha a Felhasználó kapcsolatba lép az Axionnal, support- vagy más megkeresést küld, kezelhetjük a kapcsolattartási adatokat, az üzenet és a kapcsolódó kommunikáció tartalmát, a support case azonosítóit, technikai diagnosztikai információkat, csatolmányokat, valamint a megkeresés kezeléséhez szükséges Account- vagy eseményadatokat.

Ahol az Axion analitikai vagy hasonló mérési technológiát alkalmaz, kezelhetünk a szolgáltatás használatára, oldal- vagy funkcióinterakciókra, sessionre, technikai környezetre és eseményekre vonatkozó adatokat. A cookie-k és hasonló technológiák részletes szabályait a Cookie Tájékoztató és jelen Tájékoztató vonatkozó fejezetei tartalmazzák.

2.9. Különleges adatok és más személyek adatai

Az Axion Account létrehozásához és általános használatához főszabály szerint nincs szükség a GDPR 9. cikke szerinti különleges személyes adatok megadására. A Felhasználó által biztosított tartalom, dokumentum, Connected Service adat vagy más Input azonban ilyen adatot is tartalmazhat.

A Felhasználói tartalom más természetes személyek személyes adatait is tartalmazhatja, például munkavállalók, ügyfelek, üzleti partnerek, címzettek, dokumentumokban szereplő személyek vagy más harmadik felek adatait.

Ha a Felhasználó más személy személyes adatát dolgoztatja fel az Axionnal, az adott adatkezelési helyzettől függően a Felhasználó felelhet a megfelelő jogalap, tájékoztatás és más adatvédelmi követelmények biztosításáért. A gyermekek, különleges személyes adatok, büntetőjogi adatok és harmadik személyek adatainak részletes szabályait a 12. fejezet tartalmazza.

2.10. User-operated applications adatai

Ha egy Felhasználó saját alkalmazást, workflow-t vagy más rendszert működtet Axion technológia vagy infrastruktúra használatával, az ilyen rendszer végfelhasználóira vagy más érintettjeire vonatkozó személyes adatok is feldolgozásra kerülhetnek az Axionon keresztül.

Az ilyen adatkezelésnél az adatvédelmi szerepeket a tényleges adatkezelési célok és lényeges eszközök alapján kell meghatározni. Ha a Felhasználó határozza meg az adatkezelés célját és lényeges eszközeit, a Felhasználó adatkezelő, az Axion pedig az adott feldolgozás tekintetében adatfeldolgozó lehet.

A User-operated applications részletes controller–processor modelljét a 13. fejezet és – ahol alkalmazandó – a Data Processing Agreement / Data Processing Terms tartalmazza.

3. Az adatkezelés céljai és jogalapjai

3.1. Általános jogalapi elvek

Az Axion személyes adatot kizárólag meghatározott, egyértelmű és jogszerű célból kezel, és minden adatkezeléshez az alkalmazandó adatvédelmi jog szerinti megfelelő jogalapot rendel.

A GDPR alapján az Axion adatkezelése különösen az érintett hozzájárulásán [GDPR 6. cikk (1) a)], szerződés teljesítésén vagy szerződéskötést megelőző lépéseken [6. cikk (1) b)], jogi kötelezettség teljesítésén [6. cikk (1) c)], létfontosságú érdek védelmén [6. cikk (1) d)], közérdekű vagy közhatalmi feladat teljesítésén [6. cikk (1) e)], illetve az Axion vagy harmadik fél jogos érdekén [6. cikk (1) f)] alapulhat, ha az adott jogalap feltételei ténylegesen fennállnak.

Ugyanaz a személyes adat eltérő célokból eltérő jogalapon is kezelhető. Az Axion nem tekinti egy adott célhoz fennálló jogalapot automatikus felhatalmazásnak az adat más célú kezelésére.

3.2. Account, hitelesítés és szerződéses adminisztráció

Az Account létrehozásához, a Felhasználó hitelesítéséhez, a hozzáférés biztosításához, az Account beállításainak kezeléséhez és az Axion szerződéses szolgáltatásának adminisztrációjához szükséges személyes adatokat az Axion főszabály szerint a szerződés teljesítése vagy a szerződéskötést megelőző lépések megtétele érdekében kezeli.

A jogi dokumentumok elfogadásának, verziójának és időpontjának dokumentálása, valamint egyes Account- és szerződéses nyilvántartások kezelése jogi kötelezettség vagy az Axion jogos érdeke alapján is szükséges lehet, különösen a szerződéses jogviszony, a compliance és a jogi igények igazolhatósága érdekében.

3.3. Az Axion szolgáltatás, AI-orchestration és feladatok teljesítése

Az Axion a Chat, Input, AI-modellek, orchestration, routing, tool- és agent-műveletek, Outputok, Artifacts, Projects és más alapvető szolgáltatási funkciók működtetéséhez

szükséges személyes adatokat főszabály szerint a Felhasználóval fennálló szerződés teljesítése érdekében kezeli.

Az adatkezelés célja különösen a Felhasználó utasításának értelmezése, a megfelelő modellek és eszközök kiválasztása, a feladat lépésekre bontása és koordinálása, a szükséges köztes feldolgozás elvégzése, valamint az eredmény létrehozása és a Felhasználó részére történő biztosítása.

Ha egy adott művelet nem szükséges a szerződéses szolgáltatás teljesítéséhez, az Axion arra nem hivatkozik automatikusan szerződéses jogalapként.

3.4. Fájl-, dokumentum-, research- és végrehajtási funkciók

Ha a Felhasználó fájlt vagy dokumentumot tölt fel, OCR-, webes keresési, research-, kód-, Forge-, Workflow-, sandbox- vagy más végrehajtási funkciót használ, az Axion az adott funkció működtetéséhez szükséges adatokat főszabály szerint a kért szolgáltatás teljesítése érdekében kezeli.

Az adatkezelés célja lehet különösen a dokumentum tartalmának feldolgozása, szöveg kinyerése, releváns webes vagy más külső információ felkutatása, kód vagy workflow végrehajtása, technikai eredmények előállítása és a Felhasználó által kért feladat teljesítése.

Külső forrásból származó személyes adat kezelése esetén az Axion az adatot csak az adott feladat és az alkalmazandó jog keretei között használja fel.

3.5. Connected Services, integrációk és Actions

A Felhasználó által önkéntesen összekapcsolt Connected Services és más integrációk adatainak kezelése az adott integráció biztosításához és a Felhasználó által kezdeményezett feladat vagy művelet teljesítéséhez szükséges.

Az Axion az engedélyezett hozzáférést, scope-okat, authorization adatokat és az integráción keresztül lekért vagy továbbított információt kizárólag az adott funkció működtetéséhez és a Felhasználó által kért művelethez szükséges mértékben kezeli.

Ha egy Action végrehajtása confirmationt vagy más Felhasználói jóváhagyást igényel, az Axion a jóváhagyás tényét és a kapcsolódó végrehajtási adatokat a művelet biztonságos és igazolható végrehajtása érdekében kezelheti. A confirmation nem jelent általános adatkezelési hozzájárulást más célokra.

3.6. Coin, fizetés, számlázás és elszámolás

A Coin-vásárlás, Coin-egyenleg és felhasználás, valamint a fizetés és tranzakció teljesítéséhez szükséges személyes adatokat az Axion főszabály szerint a szerződés teljesítése érdekében kezeli. Az online fizetési műveletet Stripe végzi; a számlakiállításhoz szükséges adatokat az Axion a Számlázz.hu részére továbbíthatja.

A számlakiállításhoz, adózáshoz, számvitelhez és más kötelező pénzügyi nyilvántartásokhoz kapcsolódó adatkezelés jogalapja jogi kötelezettség lehet. A számlázási adatok az alkalmazandó jogszabályok szerint a Számlázz.hu rendszerében kezelhetők, és jogszabály

alapján a könyvelő, a Nemzeti Adó- és Vámhivatal (NAV) vagy más illetékes hatóság részére hozzáférhetővé válhatnak vagy továbbításra kerülhetnek. A fraud prevention, tranzakciós visszaélések kivizsgálása és jogi igények kezelése az adott körülményektől függően az Axion jogos érdekén is alapulhat.

3.7. Support és felhasználói megkeresések

Az Axion a support-, adatvédelmi, technikai és más Felhasználói megkeresések kezeléséhez szükséges személyes adatokat a megkeresés jellegétől függően a szerződés teljesítése, jogi kötelezettség teljesítése vagy az Axion jogos érdeke alapján kezelheti.

Az adatkezelés célja különösen a kérdés vagy probléma megértése, a szükséges technikai vizsgálat, válaszadás, hibaelhárítás, panaszkezelés és a kapcsolódó kommunikáció dokumentálása.

3.8. Biztonság, fraud/abuse prevention és technikai naplózás

Az Axion a szolgáltatás, Accountok, infrastruktúra, Felhasználók és harmadik személyek biztonságának védelme érdekében személyes adatot kezelhet különösen authentication- és security monitoring, fraud- és abuse-prevention, jogosulatlan hozzáférés és támadások észlelése, incidenskezelés, hibakeresés, auditálhatóság és rendszerintegritás céljából.

Az ilyen adatkezelés főszabály szerint az Axion és adott esetben más érintettek jogos érdekein alapulhat, ha az érdekmérlegelés alapján az adatkezelés szükséges és arányos, és az érintett jogai és szabadságai nem élveznek elsőbbséget.

Ha valamely biztonsági adat kezelése jogi kötelezettség teljesítéséhez szükséges, az adott adatkezelés megfelelő jogalapja jogi kötelezettség is lehet.

3.9. Jogi igények, hatósági megkeresések és jogi kötelezettségek

Az Axion személyes adatot kezelhet az alkalmazandó jogszabályok, hatósági vagy bírósági kötelezettségek teljesítése, valamint jogi igények előterjesztése, érvényesítése vagy védelme érdekében.

Kötelező jogi előírás vagy megfelelően kötelező hatósági megkeresés esetén az adatkezelés jogalapja jogi kötelezettség lehet. Jogi igények dokumentálása, viták kezelése és az Axion jogainak védelme az adott körülményektől függően jogos érdeken is alapulhat.

Az Axion ilyen esetben is az adott jogi célhoz szükséges adatok kezelésére és átadására törekszik.

3.10. Analitika és szolgáltatáshasználat mérése

Az Axion analitikai és mérési adatokat használhat a szolgáltatás használatának megértésére, teljesítményének mérésére, hibák és használati minták azonosítására, valamint a termék működésének fejlesztésére.

Az alkalmazandó jogalap az alkalmazott technológiától és az adatkezelés jellegétől függ. Ha az adott analitikai technológia vagy cookie használatához hozzájárulás szükséges, az Axion

azt csak megfelelő hozzájárulás alapján alkalmazza. Más, megfelelően korlátozott és szükséges mérési művelet az alkalmazandó jog feltételei mellett jogos érdeken alapulhat.

3.11. Szolgáltatásfejlesztés

Az Axion a szolgáltatás megbízhatóságának, használhatóságának, teljesítményének és funkcióinak fejlesztése érdekében megfelelően korlátozott személyes adatokat kezelhet, ha ehhez megfelelő jogalap áll rendelkezésre.

Ha az adatkezelés jogos érdeken alapul, az Axion figyelembe veszi különösen az adat jellegét, az érintett észszerű elvárásait, az adatkezelés szükségességét, a lehetséges hatásokat és az alkalmazott garanciákat.

Az Axion nem tekinti a szolgáltatásfejlesztés általános célját korlátlan felhatalmazásnak a Felhasználói tartalom bármilyen további felhasználására. Ha valamely fejlesztési célhoz más jogalap, külön tájékoztatás vagy hozzájárulás szükséges, azt külön kell biztosítani.

3.12. Marketingkommunikáció

Az Axion marketing- vagy promóciós kommunikációt kizárólag az alkalmazandó elektronikus hírközlési, direkt marketing és adatvédelmi szabályok szerint küld.

A marketingkommunikáció jogalapja az adott csatornától és körülményektől függően hozzájárulás vagy más, jogszerűen alkalmazható jogalap lehet. Ahol hozzájárulás szükséges, annak megadása önkéntes, és a hozzájárulás bármikor visszavonható.

A szolgáltatás működéséhez, Account biztonságához, tranzakcióhoz, jogi változáshoz vagy más nem marketing célhoz szükséges service communication nem minősül automatikusan marketingkommunikációnak.

3.13. Hozzájárulás és jogos érdek

Ha az adatkezelés hozzájáruláson alapul, az Axion a hozzájárulást az adott célra vonatkozóan, megfelelő tájékoztatás mellett kéri. A hozzájárulás megtagadása vagy visszavonása nem érinti a visszavonás előtt, a hozzájárulás alapján végzett adatkezelés jogszerűségét.

Az ÁSZF, a Privacy Policy vagy más általános jogi dokumentum megismerése vagy elfogadása önmagában nem jelent általános GDPR-hozzájárulást minden adatkezelési célhoz.

Ha az Axion jogos érdekre támaszkodik, az adatkezelés előtt vagy annak keretében megvizsgálja a jogos érdek fennállását, az adatkezelés szükségességét, az érintettre gyakorolt hatást és az érdekek, jogok és szabadságok közötti egyensúlyt. Az érintettet a GDPR szerint tiltakozási jog illetheti meg az ilyen adatkezeléssel szemben.

3.14. Különleges helyzetek és a jogalap változása

A különleges személyes adatok, gyermekek adatai, büntetőjogi adatok, más személyekre vonatkozó Felhasználói tartalom és User-operated applications keretében végzett adatkezelések esetében további jogalapi vagy adatvédelmi követelmények alkalmazandók. Ezek részletes szabályait különösen a 12. és 13. fejezet tartalmazza.

Az Axion egy adatkezelés jogalapját nem változtatja meg pusztán jelen Tájékoztató módosításával. Ha az adatkezelés célja, körülménye vagy jogalapja érdemben megváltozik, az Axion az új adatkezelés megkezdése előtt megvizsgálja annak jogszerűségét, szükség esetén megfelelő új tájékoztatást biztosít, és ahol szükséges, új hozzájárulást vagy más megfelelő jogalapot szerez.

Jelen Tájékoztatóban valamely jogalap megjelölése nem tesz jogszerűvé olyan adatkezelést, amelyhez az adott jogalap feltételei ténylegesen nem állnak fenn.

4. Technológiai szolgáltatók, adatfeldolgozók és címzettek

4.1. Általános szabályok

Az Axion a szolgáltatás biztosításához külső technológiai, infrastruktúra-, mesterségesintelligencia-, keresési, dokumentumfeldolgozási, sandbox-, média-, hitelesítési és analitikai szolgáltatókat vehet igénybe.

E szolgáltatók adatvédelmi szerepe az adott adatkezelési művelettől, az Axion és a szolgáltató közötti szerződéses konstrukciótól, valamint attól függ, hogy ki határozza meg az adatkezelés célját és lényeges eszközeit. Egy szolgáltató ezért az adott feldolgozás körülményeitől függően adatfeldolgozóként, al-adatfeldolgozóként vagy más címzettként is megjelenhet.

Nem minden személyes adat kerül minden szolgáltatóhoz. Az Axion úgy alakítja ki az adatáramlást, hogy az adott feladat vagy funkció végrehajtásában az ahhoz szükséges szolgáltató és a szükséges adatkör vegyen részt.

4.2. AI-szolgáltatók

Az Axion AI- és orchestration-funkcióinak működtetéséhez több AI-szolgáltatót és modellt használhat. A jelenlegi szolgáltatói körbe tartozik különösen az OpenAI, az Anthropic és a Google Gemini.

Az Axion orchestration- és routing-rendszere a Felhasználó feladata, a szükséges képességek és a szolgáltatás technikai működése alapján választhatja ki, hogy az adott feladatban mely modell vagy szolgáltató vesz részt. Egy feladat végrehajtásában egy vagy több AI-szolgáltató is részt vehet.

Az AI-szolgáltató részére továbbított adatok köre az adott feladattól függhet, és tartalmazhatja különösen a feladat teljesítéséhez szükséges Inputot, kontextust, fájl- vagy dokumentumrészletet, köztes eredményt vagy más releváns információt.

4.3. Microsoft Azure infrastruktúra

Az Axion a Microsoft Azure szolgáltatásait használja vagy használhatja a szolgáltatás hostingjához, infrastruktúrájához, adatbázisaihoz és kapcsolódó technikai működéséhez, ideértve a PostgreSQL-alapú adattárolást is.

Az Azure infrastruktúrán az Axion működéséhez szükséges Account-, tartalmi, projekt-, technikai, tranzakciós, biztonsági és más szolgáltatási adatok tárolhatók vagy feldolgozhatók az adott Axion-funkciótól függően.

Az Axion az Azure konfigurációját, régióját, adatmegőrzési és biztonsági beállításait a production környezet tényleges kialakításához igazítja.

4.4. Dokumentum-, keresési-, sandbox- és médiaszolgáltatók

Az Axion egyes speciális funkciók biztosításához további technológiai szolgáltatókat használhat.

A Google dokumentumfeldolgozási vagy OCR-szolgáltatásai dokumentumokból vagy képekből történő szöveg- és adatkinyerésben vehetnek részt. A Brave Search webes keresési és research-funkciókhoz használható. Az E2B sandbox- és kódfuttatási környezetet biztosíthat. A Cloudinary média- és támogatott fájlkezelési funkciókban vehet részt.

Az adott szolgáltatóhoz kizárólag akkor kerül adat, ha az adott funkció vagy feladat ténylegesen igényli annak használatát.

4.5. Google-hitelesítés és Connected Services

A Google hitelesítési szolgáltatásának használata elkülönül a Google Gemini AI-szolgáltatástól és a Felhasználó által külön összekapcsolt Google Connected Services funkcióktól.

Google Login vagy más támogatott Google OAuth hitelesítés esetén az Axion a bejelentkezáshoz és Account-azonosításhoz szükséges adatokat és hitelesítési metaadatokat kezelheti.

Ha a Felhasználó külön összekapcsol egy támogatott Google-szolgáltatást vagy más Connected Service-t, az Axion az engedélyezett scope-ok és a Felhasználó által kezdeményezett feladat keretében férhet hozzá az adott szolgáltatás adataihoz. A hitelesítés önmagában nem jelent automatikus hozzáférést a Connected Service tartalmához.

4.6. PostHog és analitika

Az Axion PostHog szolgáltatást használhat webes vagy termékanalitika, használati események és a szolgáltatás működésének mérésére.

A PostHog részére továbbított adatok köre és az adatkezelés módja a production analitikai konfigurációtól, az alkalmazott eseményektől, cookie- vagy hasonló technológiáktól és a consent beállításoktól függ.

4.7. Adatminimalizálás és provider routing

Az Axion több szolgáltatót használó orchestration-architektúrája nem jelenti azt, hogy valamennyi provider automatikusan megkapja ugyanazt a Felhasználói tartalmat vagy személyes adatot.

Az Axion az adott feladat végrehajtásához releváns szolgáltatót választja ki, és a routingot úgy alakítja ki, hogy az adott providerhez a feladat teljesítéséhez szükséges és releváns adatkör kerüljön. Az adatáramlás a használt funkciótól, modelltől, tooltól, integrációtól és a Felhasználó utasításától függhet.

Az adatminimalizálás nem jelenti azt, hogy egy összetett feladat során személyes adat soha nem kerülhet több szolgáltatóhoz; ha több szolgáltató részvétele szükséges a kért feladat teljesítéséhez, az adat a szükséges műveletek keretében több szolgáltatónál is feldolgozásra kerülhet.

4.8. Szolgáltatói kör változása és aktuális provider-lista

Az Axion technológiai szolgáltatói, modelljei és infrastruktúra-komponensei idővel változhatnak. Egy szolgáltató vagy modell jelen Tájékoztatóban történő megnevezése nem jelenti azt, hogy az adott szolgáltató vagy modell az Axion minden funkciójában részt vesz, vagy korlátlan ideig a szolgáltatás része marad.

A jelen Tájékoztató készítésekor az Axion által használt vagy a production szolgáltatásban tervezetten használt fő technológiai szolgáltatói kör különösen:

Microsoft - Azure hosting, infrastruktúra és PostgreSQL; OpenAI - AI-modellek és API; Anthropic - Claude AI-modellek és API; Google - Gemini AI-szolgáltatás; Google - OAuth/hitelesítés és támogatott Google-integrációk; Google - dokumentumfeldolgozás/OCR; Brave - webes keresés; E2B - sandbox és kódfuttatás; Cloudinary - média- és támogatott fájlkezelés; PostHog - webes és termékanalitika; Stripe - online fizetés, payment processing és kapcsolódó tranzakciós szolgáltatások; Számlázz.hu / KBOSS.hu Kft. - számlakiállítás és kapcsolódó számlázási szolgáltatások.

Az Axion a szolgáltatói kör lényeges változása esetén jelen Tájékoztatót vagy az alkalmazandó provider/subprocessor listát megfelelően frissíti. Az adatkezelés helyére, EGT-n kívüli adattovábbításokra és alkalmazandó transfer safeguards szabályokra az 5. fejezet vonatkozik.

4.9. Axion mint adatfeldolgozó és al-adatfeldolgozók

Ha az Axion valamely Felhasználó nevében adatfeldolgozóként jár el, az Axion által az adott feldolgozáshoz igénybe vett külső szolgáltató al-adatfeldolgozóként vehet részt az adatkezelésben.

Ilyen szerep különösen az infrastruktúrát biztosító szolgáltatónál vagy az adott User-operated processing végrehajtásában ténylegesen részt vevő AI-, dokumentumfeldolgozási, sandbox- vagy más technológiai szolgáltatónál merülhet fel.

Az al-adatfeldolgozók igénybevételének, változásának, szerződéses követelményeinek és a Felhasználó mint adatkezelő jogainak részletes szabályait a 13. fejezet és – ahol alkalmazandó – a Data Processing Agreement / Data Processing Terms tartalmazza.

5. Nemzetközi adattovábbítások

5.1. Általános elvek

Az Axion európai felhasználók részére is nyújt szolgáltatást, miközben a szolgáltatás működtetéséhez nemzetközi technológiai szolgáltatókat vehet igénybe. Emiatt egyes személyes adatok az Európai Gazdasági Térségen („EGT”) kívüli országban is feldolgozásra kerülhetnek, vagy ilyen országban működő szolgáltató számára hozzáférhetővé válhatnak.

Az EGT-n kívüli adatkezelés önmagában nem jelenti azt, hogy az adattovábbítás jogellenes. Ha a GDPR V. fejezete szerinti nemzetközi adattovábbítás történik, az Axion az adott adattovábbításhoz megfelelő jogalapot, adattovábbítási mechanizmust és – ahol szükséges – további garanciákat alkalmaz.

5.2. EGT-n kívüli adatkezelés esetei

Nemzetközi adatáramlás különösen akkor fordulhat elő, ha az Axion által használt AI-, infrastruktúra-, keresési, dokumentumfeldolgozási, sandbox-, média-, analitikai vagy más technológiai szolgáltató, illetve annak al-adatfeldolgozója az EGT-n kívül végez adatkezelést vagy onnan biztosít hozzáférést.

A tényleges feldolgozási hely az adott szolgáltatótól, terméktől, contracting entitytől, választott régiótól, technikai konfigurációtól és az alkalmazott al-adatfeldolgozói lánctól függhet.

Nem minden Axion-funkció és nem minden Felhasználói adat jár nemzetközi adattovábbítással; az adatáramlás a ténylegesen használt szolgáltatástól és feldolgozási művelettől függ.

5.3. Megfelelőségi határozatok és megfelelő garanciák

Ha az Európai Bizottság az adott harmadik országra, területre, szektorra vagy megfelelő szervezeti körre vonatkozó megfelelőségi határozatot fogadott el, az adattovábbítás az alkalmazandó megfelelőségi keret alapján történhet.

Ha nincs alkalmazható megfelelőségi határozat, az Axion megfelelő garanciára támaszkodhat, ideértve különösen az Európai Bizottság által elfogadott általános szerződési feltételeket (Standard Contractual Clauses, „SCC”), ha azok az adott adattovábbításra alkalmazhatók.

Az alkalmazott mechanizmust minden esetben az adott adatáramlás, szolgáltató és szerződéses konstrukció alapján kell meghatározni.

5.4. Standard Contractual Clauses és kiegészítő intézkedések

Ha az Axion SCC-kre vagy más, megfelelő garanciát biztosító mechanizmusra támaszkodik, szükség szerint értékeli az adott adattovábbítás körülményeit és azt, hogy a fogadó ország joga vagy gyakorlata érintheti-e a garanciák tényleges érvényesülését.

Ahol az alkalmazandó jog vagy az adott adattovábbítás körülményei ezt indokolják, az Axion vagy az érintett szolgáltató további szerződéses, technikai vagy szervezési intézkedéseket alkalmazhat.

Az ilyen intézkedések jellege az adott processingtől függhet, és nem minden nemzetközi adatáramlásnál azonos.

5.5. Technológiai szolgáltatók és feldolgozási hely

A 4. fejezetben felsorolt technológiai szolgáltatók adatkezelési helye és nemzetközi adattovábbítási konstrukciója szolgáltatónként és termékenként eltérhet, továbbá idővel változhat.

Az Axion ezért a production szolgáltatásban ténylegesen használt lényeges nemzetközi adatáramlások és alkalmazandó transfer safeguards megfelelőségét a szolgáltatói és technikai konfigurációhoz igazodva kezeli.

5.6. Al-adatfeldolgozók és onward transfers

Az Axion technológiai szolgáltatói az adott szolgáltatás biztosításához további al-adatfeldolgozókat vagy infrastruktúra-szolgáltatókat vehetnek igénybe. Emiatt személyes adat az eredeti címzettől további szolgáltatóhoz is továbbításra kerülhet („onward transfer”).

Az Axion arra törekszik, hogy az általa igénybe vett adatfeldolgozói láncban a személyes adatokra megfelelő adatvédelmi kötelezettségek és – nemzetközi adattovábbítás esetén – megfelelő GDPR szerinti adattovábbítási mechanizmusok vonatkozzanak.

Az onward transfer lehetősége nem jelenti azt, hogy minden adat minden al-adatfeldolgozóhoz eljut; a tényleges adatáramlás az adott szolgáltatás és processing technikai működésétől függ.

5.7. Axion mint adatfeldolgozó

Ha az Axion valamely Felhasználó nevében adatfeldolgozóként jár el, és az adott processing során EGT-n kívüli adattovábbítás vagy al-adatfeldolgozó igénybevétele történik, az Axionnak az adatfeldolgozói láncban is biztosítania kell az alkalmazandó GDPR-követelményeknek megfelelő szerződéses és adattovábbítási keretet.

Ilyen esetben a Felhasználó lehet az adatkezelő, az Axion az adatfeldolgozó, az Axion által igénybe vett technológiai szolgáltató pedig az adott feldolgozás tekintetében al-adatfeldolgozó.

Az ilyen feldolgozások nemzetközi adattovábbítására és al-adatfeldolgozóira vonatkozó részletes kötelezettségeket a 13. fejezet és – ahol alkalmazandó – a Data Processing Agreement / Data Processing Terms tartalmazza.

5.8. Változások, átláthatóság és további információ

A nemzetközi adattovábbítások jogi és technikai környezete, a szolgáltatói lánc és az alkalmazható transfer mechanism idővel változhat.

Ha egy korábban alkalmazott adattovábbítási mechanizmus érvényét veszti, az adott adatáramlásra nem alkalmazható többé, vagy más okból nem biztosít megfelelő védelmet, az Axion megfelelő alternatív mechanizmust vagy további garanciát alkalmaz, illetve szükség esetén az érintett adatáramlást módosítja, korlátozza vagy megszünteti.

Az érintett a rá vonatkozó nemzetközi adattovábbításokkal és az alkalmazott megfelelő garanciákkal kapcsolatban további tájékoztatást kérhet az Axiontól a support@axionaiapp.com e-mail-címen. Ahol az alkalmazandó jog ezt biztosítja, az érintett megfelelő módon információt vagy másolatot kérhet az alkalmazott garanciákról, az üzleti titkok és más személyek jogainak megfelelő védelme mellett.

6. Megőrzés és törlés

6.1. Általános megőrzési elvek

Az Axion a személyes adatokat főszabály szerint csak addig őrzi meg, ameddig az adott adatkezelési cél teljesítéséhez, a szolgáltatás biztosításához, jogi kötelezettség teljesítéséhez, biztonsági célhoz vagy jogi igény érvényesítéséhez szükséges.

A megőrzési idő meghatározásakor az Axion figyelembe veszi különösen az adat jellegét, az adatkezelés célját és jogalapját, a Felhasználó által végzett törlési műveleteket, az alkalmazandó jogi kötelezettségeket, valamint a technikai rendszerek és külső szolgáltatók működését.

A törlés nem minden esetben jelent azonnali és egyidejű fizikai eltávolítást valamennyi aktív rendszerből, backupból és külső szolgáltatói környezetből. Az Axion a törlési folyamatokat a jelen fejezetben meghatározott szabályok szerint hajtja végre.

6.2. Account és szolgáltatási adatok

Az aktív Account működéséhez szükséges Account-, profil-, hitelesítési, beállítási és szolgáltatási adatokat az Axion főszabály szerint az Account fennállásáig, illetve az adott funkció biztosításához szükséges ideig kezeli.

Egyes szerződéses, tranzakciós, biztonsági, audit- vagy jogi adatok az Account megszűnését követően is megőrizhetők, ha erre alkalmazandó jogi kötelezettség, jogi igény, fraud- vagy abuse-prevention, biztonsági incidens kezelése vagy más megfelelő jogalap miatt szükség van.

Az ilyen kivételes megőrzés nem jelenti azt, hogy az Axion a törölt Account teljes tartalmát korlátlan ideig megőrzi.

6.3. Chat, Projects, Artifacts, fájlok és más Felhasználói tartalom törlése

Ha a Felhasználó az Axionban olyan tartalmat töröl, amelyhez a szolgáltatás törlési funkciót biztosít, az Axion a törlési folyamatot a Felhasználó kérésének megfelelően megkezdi.

A törölt Chat, Project, Artifact, fájl vagy más kapcsolódó Felhasználói tartalom az aktív felhasználói környezetből eltávolításra kerülhet, majd a kapcsolódó backend- és tárolórendszerekből a technikai törlési folyamat szerint kerül végleges eltávolításra.

A jelenlegi Axion-rendszerben az ilyen törlési folyamat célzott maximális időtartama legfeljebb 30 nap, kivéve, ha az adat további megőrzését alkalmazandó jogi kötelezettség, jogi igény, biztonsági ok vagy más, jelen Tájékoztatóban meghatározott kivétel indokolja.

6.4. Account törlése és a legfeljebb 30 napos törlési folyamat

Account törlése esetén az Axion megkezdi az Account és az ahhoz kapcsolódó, további megőrzést nem igénylő személyes adatok törlését vagy anonimizálását.

A jelenlegi rendszer kialakítása szerint az Account törléséhez kapcsolódó törlési folyamat legfeljebb 30 napon belül lezárul az Axion aktív rendszereiben és a törlési folyamat hatálya alá tartozó adattárolókban, a technikailag szükséges feldolgozási idő figyelembevételével.

A 30 napos időablak nem írja felül azokat az eseteket, amikor az Axion valamely adatot jogszabály alapján köteles tovább megőrizni, vagy megfelelő jogalap alapján jogi igény, biztonsági incidens, fraud/abuse investigation vagy más kivételes cél miatt szükséges ideig megőrizhet.

6.5. Backupok és technikai maradványadatok

A személyes adatok biztonsági mentésekben, disaster-recovery rendszerekben vagy más technikai másolatokban az aktív rendszerből történő törlést követően korlátozott ideig tovább fennmaradhatnak.

Az ilyen backup-adatok rendeltetése a rendszer helyreállíthatóságának és üzembiztonságának biztosítása. A backupokban fennmaradó, az aktív rendszerekből már törölt személyes adatot az Axion nem használja új, önálló adatkezelési célra; az ilyen adat kizárólag a backup és disaster-recovery funkcióhoz szükséges ideig maradhat fenn, majd a backup életciklusának megfelelően törlésre vagy felülírásra kerül.

Ha backup-helyreállítás következtében korábban törölt személyes adat technikailag ismét megjelenik, az Axion megfelelő eljárással ismét érvényesíti a korábbi törlési állapotot, kivéve, ha az adat további megőrzésére megfelelő jogalap áll fenn.

6.6. Jogi, pénzügyi, biztonsági és jogérvényesítési kivételek

Bizonyos személyes adatokat az Axion a Felhasználó által kezdeményezett törlés vagy Account megszűnése után is köteles vagy jogosult lehet megőrizni.

Ide tartozhatnak különösen a számviteli, adózási és számlázási nyilvántartások; a szerződés és jogi dokumentumok elfogadásának bizonyítékai; hatósági vagy bírósági kötelezettséghez szükséges adatok; jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez szükséges információk; valamint a security, fraud- vagy abuse-események megfelelő kivizsgálásához és dokumentálásához szükséges adatok. A Számlázz.hu rendszerében kezelt

számlák és kötelező számviteli vagy adózási adatok ezért nem tartoznak automatikusan az Axion általános, legfeljebb 30 napos törlési folyamatának hatálya alá.

Az Axion az ilyen adatokat csak az adott kivételes célhoz szükséges körben és időtartamig őrzi meg, és nem kezeli őket tovább az eredeti, már megszűnt szolgáltatási célra, ha ahhoz nincs külön megfelelő jogalap.

6.7. Külső szolgáltatók és provider-side retention

Ha személyes adat az Axion által igénybe vett technológiai szolgáltatóhoz kerül, annak törlése és megőrzése részben az adott provider technikai és szerződéses adatkezelési mechanizmusaitól is függhet.

Az Axion saját rendszerében végrehajtott törlés ezért nem minden esetben jelenti azt, hogy az adat ugyanabban a pillanatban minden külső szolgáltatói rendszerből, ideiglenes tárolóból, biztonsági mentésből vagy naplóból is fizikailag eltűnik.

Az Axion arra törekszik, hogy olyan szolgáltatói és szerződéses konstrukciókat alkalmazzon, amelyek megfelelő törlési és megőrzési szabályokat biztosítanak, és ahol az Axionnak erre lehetősége vagy kötelezettsége van, a szükséges provider-side törlési folyamatokat kezdeményezi vagy érvényesíti.

A provider-specifikus retention időtartam a szolgáltatótól, terméktől, konfigurációtól, az adott adatáramlástól és az alkalmazandó jogi kötelezettségektől függhet. Ez különösen releváns lehet a Stripe fizetési/tranzakciós processingje és a Számlázz.hu számlázási, számviteli és adózási nyilvántartásai esetében.

6.8. Axion mint adatfeldolgozó

Ha az Axion valamely Felhasználó nevében adatfeldolgozóként jár el, a User-operated processing keretében kezelt személyes adatok megőrzésére és törlésére elsősorban az adatkezelő Felhasználó dokumentált utasításai, az alkalmazandó Data Processing Agreement / Data Processing Terms és a GDPR adatfeldolgozókra vonatkozó szabályai irányadók.

Az Axion az ilyen adatok törlését vagy visszaadását az alkalmazandó adatfeldolgozási feltételek szerint végzi, kivéve, ha uniós vagy tagállami jog az adatok további megőrzését írja elő.

Az Axion saját, elkülönült adatkezelői céljaihoz – például Account-, számlázási, biztonsági vagy jogi megfelelési célból – kezelt adatok megőrzésére továbbra is az Axion adatkezelőként alkalmazott megőrzési szabályai vonatkoznak.

7. Az érintettek jogai és kérelmek kezelése

7.1. Általános szabályok

Az érintettet az alkalmazandó adatvédelmi jog, különösen a GDPR alapján az e fejezetben ismertetett jogok illethetik meg. A jogok gyakorlása az adott adatkezelés körülményeitől és a GDPR-ban meghatározott feltételektől függ.

Az érintett kérelmét az Axion részére különösen a support@axionaiapp.com e-mail-címen nyújthatja be. Az Axion a kérelmet indokolatlan késedelem nélkül, főszabály szerint annak beérkezésétől számított egy hónapon belül kezeli. A GDPR-ban meghatározott esetekben ez a határidő további két hónappal meghosszabbítható; ilyen esetben az Axion az első egy hónapon belül tájékoztatja az érintettet a hosszabbításról és annak okairól.

A kérelmek teljesítése főszabály szerint díjmentes. Nyilvánvalóan megalapozatlan vagy – különösen ismétlődő jellegük miatt – túlzó kérelmek esetén az Axion a GDPR által megengedett módon és feltételekkel észszerű díjat számíthat fel vagy megtagadhatja a kérelem teljesítését.

Ha az Axionnak megalapozott kétsége van a kérelmet benyújtó személy személyazonosságával kapcsolatban, kizárólag a személyazonosság megerősítéséhez szükséges további információt kérhet. Az Axion nem követeli meg automatikusan személyazonosító okmány benyújtását minden érintetti kérelemhez.

7.2. Hozzáféréshez való jog

Az érintett jogosult visszajelzést kérni arról, hogy az Axion kezeli-e a rá vonatkozó személyes adatokat, és ha igen, hozzáférést kérhet a személyes adatokhoz és a GDPR szerint biztosítandó kapcsolódó információkhoz.

A hozzáférési jog az Axionban kezelt Account-, Chat-, Input-, Output-, Artifact-, Project-, Connected Service-, support-, technikai vagy más személyes adatra is kiterjedhet, amennyiben az adott információ az érintettre vonatkozó személyes adat és az Axion adatkezelőként kezeli.

A másolat biztosítása során az Axion figyelembe veszi más személyek jogait és szabadságait, valamint az alkalmazandó jog által védett titkokat és biztonsági érdekeket.

7.3. Helyesbítéshez való jog

Az érintett kérheti a rá vonatkozó pontatlan személyes adatok helyesbítését, illetve – az adatkezelés célját figyelembe véve – a hiányos személyes adatok kiegészítését.

Ha az adatot a Felhasználó saját maga módosíthatja az Axion megfelelő felületén, az Axion erre a lehetőségre is felhívhatja a figyelmet, de ez nem szünteti meg az érintett GDPR szerinti jogát, ha annak feltételei fennállnak.

7.4. Törléshez való jog

Az érintett a GDPR-ban meghatározott esetekben kérheti a rá vonatkozó személyes adatok törlését. A törléshez való jog nem korlátlan; az Axion megtagadhatja vagy korlátozhatja a törlést, ha az adat további kezelése például jogi kötelezettség teljesítéséhez, jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, illetve más GDPR szerinti kivétel miatt szükséges.

Az Axion felületén végzett Account-, Chat-, Project-, Artifact-, fájl- vagy más tartalomtörlés termékfunkcióként elindíthatja a kapcsolódó technikai törlési folyamatot. Az érintett ettől függetlenül külön GDPR szerinti törlési kérelmet is benyújthat.

Egy GDPR szerinti törlési kérelem nem jelent szükségszerűen teljes Account-törlést, ha a kérelem csak meghatározott adatra vagy adatkezelésre vonatkozik. A törlési folyamat technikai és megőrzési szabályait a 6. fejezet részletezi.

7.5. Az adatkezelés korlátozásához való jog

Az érintett a GDPR-ban meghatározott esetekben kérheti személyes adatai kezelésének korlátozását, például ha vitatja az adatok pontosságát, az adatkezelés jogellenes, de ellenzi a törlést, az Axionnak már nincs szüksége az adatra, de az érintett jogi igényhez igényli azt, vagy az érintett tiltakozott az adatkezelés ellen és az érdekmérlegelés még folyamatban van.

Korlátozás esetén az Axion az adatot – a tárolás kivételével – csak a GDPR által megengedett feltételek mellett kezeli tovább.

7.6. Adathordozhatósághoz való jog

Ha a GDPR feltételei fennállnak, az érintett jogosult az általa az Axion rendelkezésére bocsátott, rá vonatkozó személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapni, és jogosult lehet ezen adatok más adatkezelő részére történő továbbítására.

Az adathordozhatóság különösen a hozzájáruláson vagy szerződésen alapuló, automatizált módon végzett adatkezelésre vonatkozhat. A jog nem jelenti automatikusan az Axion valamennyi belső technikai adatának, következtetésének, rendszerinformációjának vagy más személy jogait érintő adatának exportálhatóságát.

7.7. Tiltakozáshoz való jog

Az érintett a saját helyzetével kapcsolatos okból tiltakozhat a GDPR 6. cikk (1) e) vagy f) pontján alapuló adatkezeléssel szemben. Ilyen esetben az Axion a személyes adatot nem kezeli tovább, kivéve, ha bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódik.

Ha személyes adat kezelése közvetlen üzletszerzés céljából történik, az érintett bármikor tiltakozhat az ilyen célú adatkezeléssel szemben; ilyen tiltakozás esetén a személyes adat a továbbiakban közvetlen üzletszerzés céljából nem kezelhető.

7.8. Hozzájárulás visszavonása

Ha valamely adatkezelés hozzájáruláson alapul, az érintett a hozzájárulását bármikor visszavonhatja. A visszavonás nem érinti a visszavonás előtt, a hozzájárulás alapján végzett adatkezelés jogszerűségét.

Az ÁSZF, jelen Tájékoztató vagy más általános jogi dokumentum elfogadása vagy megismerése önmagában nem minősül általános adatkezelési hozzájárulásnak.

7.9. Automatizált döntéshozatal és AI

Az Axion AI-modelleket, orchestrationt, routingot és automatizált technikai folyamatokat használ a szolgáltatás működtetéséhez és a Felhasználó által kért Outputok létrehozásához.

Az AI által generált Output, modellválasztás, routing vagy más automatizált technikai művelet önmagában nem feltétlenül minősül a GDPR 22. cikke szerinti, kizárólag automatizált adatkezelésen alapuló olyan döntésnek, amely az érintettre nézve joghatással jár vagy őt hasonlóképpen jelentős mértékben érinti.

Ha az Axion olyan adatkezelést vezetne be, amelyre a GDPR 22. cikke alkalmazandó, az Axion biztosítja az alkalmazandó jog által megkövetelt tájékoztatást és garanciákat, ideértve – ahol releváns – az emberi beavatkozás kérésének, az álláspont kifejtésének és a döntés vitatásának lehetőségét.

7.10. Címzettek, adatfeldolgozók és processor-helyzetek

Ha az Axion helyesbítési, törlési vagy korlátozási kérelmet teljesít, a GDPR által előírt esetekben tájékoztatja azokat a címzetteket, akikkel az érintett személyes adatát közölte, kivéve, ha ez lehetetlennek bizonyul vagy aránytalanul nagy erőfeszítést igényel. Az érintett kérésére az Axion tájékoztatást adhat e címzettekről a GDPR keretei között.

Az érintetti kérelem technikai teljesítéséhez szükség lehet az Axion adatfeldolgozóinak vagy más technológiai szolgáltatóinak bevonására.

Ha az Axion valamely User-operated processing tekintetében kizárólag adatfeldolgozóként jár el, az érintetti kérelem elsődleges címzettje az adatkezelő Felhasználó. Az Axion a GDPR, a dokumentált utasítások és az alkalmazandó Data Processing Agreement / Data Processing Terms szerint segítséget nyújt az adatkezelőnek a kérelem teljesítésében.

7.11. Más személyek jogai, képviselet és kiskorú érintettek

Ha egy Axionban kezelt dokumentum, Input, Connected Service adat, User-operated application vagy más tartalom harmadik személy személyes adatát tartalmazza, az érintett jogai az adott adatkezelési szerepek szerint gyakorolhatók.

Az érintett megfelelő meghatalmazással képviselő útján is eljárhat. Az Axion a képviseleti jogosultság igazolásához a szükséges információt kérheti.

Az Axion szolgáltatásának használatára vonatkozó korhatár nem zárja ki, hogy egy Felhasználó által feldolgozott tartalom kiskorú személyes adatát tartalmazza. Ilyen esetben az érintetti jogok és az esetleges képviselet kérdését az alkalmazandó adatvédelmi szabályok szerint kell kezelni.

7.12. Panasz és bírósági jogorvoslat

Az érintett jogosult panaszt tenni az illetékes adatvédelmi felügyeleti hatóságnál, különösen a szokásos tartózkodási helye, munkahelye vagy a feltételezett jogsértés helye szerinti tagállamban, ha úgy véli, hogy személyes adatainak kezelése sérti a GDPR-t.

Az érintett a GDPR-ban és más alkalmazandó jogszabályokban meghatározott feltételek szerint bírósági jogorvoslatra is jogosult.

Az érintett a panasz benyújtása előtt is kapcsolatba léphet az Axionnal a support@axionaiapp.com címen, hogy az Axion megvizsgálhassa és lehetőség szerint rendezhesse a felmerült adatvédelmi kérdést. Ez nem korlátozza az érintett hatósági vagy bírósági jogorvoslati jogát.

7.13. Kérelmek dokumentálása és technikai teljesítése

Az Axion az érintetti kérelmek beérkezését, kezelését és teljesítését a GDPR-megfelelés, biztonság, auditálhatóság és jogi igények kezelése érdekében megfelelően dokumentálhatja.

A kérelmek teljesítése során az Axion megfelelő technikai és szervezési intézkedéseket alkalmaz annak érdekében, hogy a személyes adat ne kerüljön jogosulatlan személyhez, és a kérelem ne veszélyeztesse más érintettek jogait vagy a szolgáltatás biztonságát.

Az Axion belső termék-, backend- vagy provider-folyamatai nem korlátozhatják az érintettet a GDPR alapján ténylegesen megillető jogok gyakorlásában. A technikai végrehajtás módját az Axion az adott kérelemhez és rendszerhez igazítja.

8. Google-szolgáltatások, OAuth és Connected Google Services

8.1. A Google-szolgáltatások eltérő szerepei

Az Axion több, egymástól eltérő Google-szolgáltatást használhat. A Google-fiókkal történő bejelentkezés, a Google Gemini AI-szolgáltatás, a dokumentumfeldolgozási/OCR-funkciók és a Felhasználó által külön összekapcsolt Google-szolgáltatások eltérő adatkezelési műveletek.

A Google-fiókkal történő bejelentkezés önmagában nem biztosít az Axion számára hozzáférést a Felhasználó Gmail-, Google Drive-, Google Calendar- vagy más Connected Google Service tartalmához.

Az Axion csak akkor fér hozzá ilyen szolgáltatás adataihoz, ha a Felhasználó az adott integrációt külön összekapcsolja, a szükséges jogosultságokat engedélyezi, és az adott funkció vagy Felhasználói kérés ténylegesen igényli a hozzáférést.

8.2. Google Login és OAuth-hitelesítés

Ha a Felhasználó Google-fiókkal jelentkezik be az Axionba, az Axion a hitelesítéshez és az Account azonosításához szükséges adatokat kaphatja meg a Google-től, például a Felhasználó nevét, e-mail-címét, profilinformációját, provider-azonosítóját és kapcsolódó hitelesítési metaadatokat, az adott OAuth-konfigurációtól függően.

A Google Login célja az authentication és Account-hozzáférés biztosítása. Az authentication során megadott jogosultság nem értelmezhető automatikusan más Google-szolgáltatások tartalmához adott hozzáférésként.

Az Axion a hitelesítési adatokat a 2., 3. és 6. fejezetben meghatározott adatkezelési és megőrzési szabályok szerint kezeli.

8.3. Connected Google Services és külön authorization

A Gmail, Google Drive, Google Calendar vagy más támogatott Google-szolgáltatás Axionhoz történő összekapcsolása külön authorization folyamatot igényelhet.

Az Axion az adott integráció működéséhez szükséges OAuth scope-okra korlátozza a kért hozzáférést. Ha egy később használt funkció további jogosultságot igényel, az Axion további vagy incremental authorizationt kérhet a Felhasználótól.

A Felhasználó dönthet arról, hogy az adott Connected Google Service-t összekapcsolja-e az Axionnal. Az integráció hiánya az adott Google-funkció használatát korlátozhatja, de önmagában nem akadályozza az Axion más, integrációt nem igénylő funkcióinak használatát.

8.4. Gmail, Google Drive, Google Calendar és más támogatott szolgáltatások

A ténylegesen elérhető Google-integrációk és funkciók a production konfigurációtól függnek.

Gmail-integráció használatakor az Axion a Felhasználó által engedélyezett scope és kezdeményezett feladat keretében e-mailekhez, threadekhez, címzettekhez, tárgyhoz, üzenettartalomhoz, csatolmányokhoz vagy kapcsolódó metaadatokhoz férhet hozzá, illetve támogatott esetben e-maillel kapcsolatos műveletet hajthat végre.

Google Drive-integráció esetén az Axion a szükséges jogosultságok keretében fájlokhoz, dokumentumokhoz, fájlnevekhez, tartalomhoz és kapcsolódó metaadatokhoz férhet hozzá a Felhasználó által kért feladat teljesítéséhez.

Google Calendar-integráció esetén az Axion a szükséges jogosultságok keretében naptáreseményekhez, időpontokhoz, résztvevőkhöz, leírásokhoz és más kapcsolódó eseményadatokhoz férhet hozzá, illetve támogatott esetben naptárműveletet hajthat végre.

Az Axion nem feltételezi, hogy egy Connected Google Service teljes tartalma szükséges egy feladathoz; az adatkezelés az engedélyezett scope-okhoz és a tényleges Felhasználói kéréshez igazodik.

8.5. Google Actions és confirmation

A Google-adatok lekérése vagy elemzése és egy külső hatással járó Google-művelet végrehajtása eltérő művelet lehet.

Ha az Axion olyan támogatott Actiont hajt végre, amely például e-mail küldését, naptáresemény létrehozását vagy módosítását, fájlműveletet vagy más külső változtatást eredményez, a szolgáltatás az adott művelet jellegétől függően confirmationt vagy más Felhasználói jóváhagyást kérhet.

A confirmation az adott művelet végrehajtására vonatkozik, és nem jelent általános hozzájárulást a Google-adatok más célú kezeléséhez.

8.6. Google API User Data és Limited Use

Az Axion a Google API-kon keresztül kapott Felhasználói adatokat kizárólag az engedélyezett funkciók biztosításához, a Felhasználó által kért feladatok teljesítéséhez, a szükséges biztonsági és működési célokhoz, valamint az alkalmazandó jogi kötelezettségek teljesítéséhez használja.

Az Axion a Google API User Data kezelésénél alkalmazza a rá vonatkozó Google API Services User Data Policy és Limited Use követelményeket, amennyiben azok az adott szolgáltatásra, scope-ra és adatkezelésre alkalmazandók.

Az Axion a Google API-kon keresztül megszerzett Google API User Data-t nem értékesíti, nem használja hirdetési vagy retargeting célra, és nem továbbítja data broker részére.

Az Axion nem használja a Google API-kon keresztül kapott adatokat olyan célra, amely összeegyeztethetetlen a Felhasználó által engedélyezett funkcióval vagy az alkalmazandó Google API követelményekkel.

8.7. Google API adatok és AI-feldolgozás

Ha a Felhasználó olyan Axion-feladatot kezdeményez, amelynek teljesítéséhez egy Connected Google Service-ből származó adat AI-feldolgozása szükséges, az Axion a feladat teljesítéséhez szükséges adatot az orchestration folyamatban ténylegesen részt vevő megfelelő AI-szolgáltatóhoz továbbíthatja.

Ilyen feldolgozás például akkor lehet szükséges, ha a Felhasználó e-mail összefoglalását, dokumentum elemzését, naptárinformáció értelmezését vagy más, Google-adaton alapuló AI-feladatot kér.

Ha a Felhasználó által kért funkció teljesítéséhez szükséges, a Connected Service-ből származó releváns Google API User Data az Axion által az adott feladathoz kiválasztott AI- vagy más technológiai szolgáltató részére továbbításra kerülhet. Az Axion az ilyen továbbítást

a feladat teljesítéséhez szükséges és releváns adatkörre korlátozza. Az AI-szolgáltatókra, provider routingra és nemzetközi adattovábbításokra a 4. és 5. fejezet szabályai irányadók.

8.8. Tokenek, biztonság, visszavonás és leválasztás

Az Axion a Connected Google Services működtetéséhez szükséges access tokeneket, refresh tokeneket vagy más authorization adatokat kezelhet. Ezeket az Axion biztonsági szempontból érzékeny hitelesítési adatként kezeli, és megfelelő technikai és szervezési intézkedésekkel védi.

A Felhasználó az Axion által biztosított funkción vagy a Google megfelelő account- és security-beállításain keresztül visszavonhatja a hozzáférést vagy leválaszthatja az integrációt, az adott szolgáltatás technikai lehetőségeitől függően.

A hozzáférés visszavonását vagy az integráció leválasztását követően az Axion nem használhatja tovább az érvényét vesztett authorizationt új Google API-hozzáférésre. A korábban jogszerűen feldolgozott adatok további megőrzésére a 6. fejezet szabályai vonatkoznak.

8.9. Megőrzés és törlés

A Connected Google Service leválasztása vagy az OAuth-hozzáférés visszavonása megszünteti vagy korlátozza az Axion jövőbeli hozzáférését az adott Google-szolgáltatáshoz, de nem feltétlenül jelenti minden korábban feldolgozott adat, létrehozott Output vagy Artifact azonnali törlését.

A Google API-ból származó, az Axion rendszereiben megőrzött személyes adatok törlésére, Account- és tartalomtörlésre, backupokra és jogi kivételekre a 6. fejezet vonatkozik.

Ha az Axion az adott Google-adatot valamely Felhasználó nevében adatfeldolgozóként kezeli, a törlésre az adatkezelő utasításai és az alkalmazandó Data Processing Agreement / Data Processing Terms is irányadó lehet.

8.10. Felhasználói kontroll, Google Workspace és megosztott Accountok

A Felhasználó felel azért, hogy csak olyan Google-fiókot és Google-adatot kapcsoljon az Axionhoz, amelyhez megfelelő jogosultsággal rendelkezik, és hogy az engedélyezett scope-okat az authorization során áttekintse.

Google Workspace vagy más szervezeti fiók esetén a szervezet adminisztrátora további hozzáférési, alkalmazás- vagy API-korlátozásokat alkalmazhat. Ezek befolyásolhatják, hogy az Axion mely Google-integrációkat és funkciókat tudja biztosítani.

Ha ugyanahhoz az Axion Accounthoz több személy fér hozzá, az Accounttal összekapcsolt Google-adatokhoz és az azokból létrehozott Outputokhoz való hozzáférés kockázata növekedhet. Az Account jogosult használóinak és hozzáféréseinek megfelelő kezelése ezért különösen fontos.

8.11. Google API compliance és változások

Az Axion a Google API-k és OAuth-funkciók használatát az alkalmazandó Google developer, OAuth, API User Data és más releváns követelményekhez igazítja.

Az elérhető Google-integrációk, kért scope-ok, consent- és authorization flow-k, valamint a Google által előírt verification vagy más compliance követelmények idővel változhatnak. Az Axion ennek megfelelően módosíthatja az integráció technikai működését, az engedélykérést vagy jelen Tájékoztatót.

9. AI-szolgáltatók, orchestration és AI-adatkezelés

9.1. AI-architektúra és orchestration

Az Axion több AI-szolgáltatót és modellt használhat a Felhasználó által kért feladatok teljesítéséhez. A jelenlegi fő AI-szolgáltatói körbe különösen az OpenAI, az Anthropic és a Google Gemini tartozik.

Az Axion orchestration- és routing-rendszere a feladat jellege, a szükséges képességek, a technikai elérhetőség, a biztonsági és adatvédelmi követelmények, valamint más releváns működési szempontok alapján választhatja ki az adott feladatban részt vevő modellt vagy szolgáltatót.

Az orchestration nem jelenti azt, hogy minden Felhasználói adat automatikusan minden AI-szolgáltatóhoz eljut. Egy feladatban egy vagy több AI-szolgáltató vehet részt, a tényleges feladatvégrehajtási útvonaltól függően.

9.2. Az AI-feldolgozás célja és jogalapja

Az AI-feldolgozás elsődleges célja a Felhasználó által kezdeményezett feladat értelmezése, végrehajtása és a kért Output létrehozása, ideértve szükség szerint az elemzést, összefoglalást, kutatást, tartalom- vagy kódgenerálást, dokumentumfeldolgozást, döntéstámogató eredmények előállítását és más támogatott AI-funkciókat.

Az ilyen adatkezelés főszabály szerint a Felhasználóval fennálló szerződés teljesítéséhez kapcsolódik, amennyiben az adott AI-feldolgozás a Felhasználó által kért szolgáltatás biztosításához szükséges. Más célú AI-adatkezeléshez külön megfelelő jogalap szükséges.

Az AI-feldolgozás részletes jogalapi szabályaira a 3. fejezet irányadó.

9.3. AI-szolgáltatóhoz továbbítható adatok

Az adott AI-feladat teljesítéséhez szükséges mértékben az AI-szolgáltatóhoz továbbítható különösen a Felhasználó Inputja, a releváns beszélgetési vagy feladatkontextus, feltöltött fájl vagy dokumentum szükséges része, Connected Service-ből származó releváns adat, kutatási vagy tool-eredmény, köztes orchestration-eredmény, valamint más, a feladat végrehajtásához szükséges információ.

Az Axion nem tekinti az Accountban, Projectben, Connected Service-ben vagy más rendszerben elérhető teljes adatkört automatikusan szükséges AI-inputnak. A továbbított adatok köre az adott feladat és a tényleges processing útvonal alapján változhat.

A személyes adatok AI-szolgáltatóhoz történő továbbítása az adott szolgáltató adatvédelmi szerepétől és processing konstrukciójától függően adatfeldolgozói, al-adatfeldolgozói vagy más címzetti adatkezelést eredményezhet.

9.4. Adatminimalizálás, routing és többmodell-feldolgozás

Az Axion az AI-feldolgozás során az adott modellhez vagy szolgáltatóhoz továbbított adatot a feladat teljesítéséhez szükséges és releváns adatkörre korlátozza.

Összetett feladat esetén az orchestration a feladatot több lépésre bonthatja, és eltérő lépésekhez eltérő AI-modelleket, toolokat vagy szolgáltatókat rendelhet. Emiatt ugyanazon feladat különböző részei különböző providereknél kerülhetnek feldolgozásra.

Az adatminimalizálás nem jelent abszolút garanciát arra, hogy egy összetett feladatban személyes adat csak egyetlen providerhez kerül; azt jelenti, hogy az Axion az adatáramlást a tényleges feladatvégrehajtáshoz szükséges körre korlátozza, és nem broadcastolja automatikusan a teljes Felhasználói tartalmat valamennyi elérhető AI-szolgáltató felé.

9.5. Provider-side adatkezelés és retention

Az AI-szolgáltatók a részükre továbbított adatokat saját technikai rendszereikben az Axionnal fennálló szerződéses, termék- és API-feltételek, konfigurációk, biztonsági mechanizmusok és alkalmazandó jogi kötelezettségek szerint dolgozhatják fel.

Az Axion saját megőrzési és törlési szabályai és az AI-szolgáltató technikai retention mechanizmusai elkülönülhetnek. Az Axion rendszerében történő törlés ezért nem minden esetben jelenti ugyanabban a pillanatban a provider valamennyi technikai rendszerében fennálló másolat eltűnését, és a provider-side retention megszűnése sem jelenti automatikusan az Axionban megőrzött Output vagy Artifact törlését.

Az Axion provider-specifikus retention időt, Zero Data Retention státuszt, regionális processinget vagy más különleges adatkezelési garanciát csak akkor kezel konkrét szolgáltatási ígéretként, ha azt a tényleges production API, konfiguráció és szerződéses feltételek megfelelően alátámasztják.

9.6. Model training, service improvement és provider feedback

Jelen Tájékoztató nem ad általános felhatalmazást az AI-szolgáltatóknak arra, hogy az Axionon keresztül továbbított Felhasználói tartalmat saját általános modelltraining céljukra használják.

Az, hogy egy adott AI-szolgáltató milyen mértékben használhat API-adatot modellfejlesztésre, service improvementre, abuse monitoringra, feedback feldolgozására vagy más provider-side célra, az adott production terméktől, szerződéses feltételektől,

konfigurációtól és a Felhasználó vagy az Axion által esetlegesen kezdeményezett külön funkciótól függ.

Az Axion nem tekinti a „no training”, Zero Data Retention vagy hasonló provider-állítást automatikusan minden termékre és processingre alkalmazandónak. Ilyen konkrét állítás csak ellenőrzött szerződéses és technikai alap alapján tehető.

Ha az Axion olyan feedback-funkciót biztosít, amelynek használata további adat providerhez történő továbbításával járhat, az ilyen adatáramlást az adott funkció és az alkalmazandó provider-feltételek szerint kell kezelni.

9.7. Connected Service és különleges adatok AI-feldolgozása

Connected Service-ből származó adat csak akkor kerülhet AI-feldolgozásba, ha az adott Felhasználói feladat ezt ténylegesen igényli, és a szükséges hozzáférés és authorization rendelkezésre áll. A Google API adatok AI-feldolgozására a 8. fejezet további szabályai irányadók.

Az Axion Account létrehozásához és általános használatához főszabály szerint nincs szükség különleges személyes adatok megadására. A Felhasználó által biztosított Input, dokumentum, Connected Service adat vagy más tartalom azonban ilyen adatot is tartalmazhat, amely az adott AI-feladat részeként feldolgozásra kerülhet.

A különleges személyes adatokra, más személyek adataira és kapcsolódó korlátozásokra a 12. fejezet szabályai irányadók.

9.8. Security, abuse monitoring és provider access

Az AI-szolgáltatók a szolgáltatás biztonsága, abuse- és fraud-prevention, incidenskezelés, hibakeresés, support vagy jogi kötelezettség teljesítése érdekében korlátozott technikai vagy emberi hozzáférést alkalmazhatnak, ha ezt az adott provider terméke, szerződése és alkalmazandó szabályai lehetővé teszik.

Az Axion arra törekszik, hogy production környezetben olyan provider- és konfigurációs megoldásokat használjon, amelyek az adott use case-hez megfelelő adatvédelmi és biztonsági garanciákat biztosítanak.

A provider-side security vagy abuse processing nem értelmezhető automatikusan az Axion által adott általános felhatalmazásként a Felhasználói tartalom tetszőleges további felhasználására.

9.9. AI-provider változások és vendor governance

Az Axion idővel új AI-szolgáltatót vagy modellt vezethet be, meglévő modellt cserélhet, korlátozhat vagy megszüntethet, illetve módosíthatja az orchestration routingját.

Egy provider vagy modell változása önmagában nem feltétlenül igényli jelen Tájékoztató teljes újraszabályozását, ha az új processing továbbra is megfelel a jelen Tájékoztatóban vállalt adatvédelmi elveknek és az alkalmazandó jognak. Lényeges adatkezelési változás esetén az Axion megfelelően frissíti a tájékoztatást.

Az Axion a production AI-provider körre vonatkozó lényeges adatvédelmi, szerződéses, retention-, security-, subprocessor- és nemzetközi adattovábbítási információkat megfelelő belső vendor governance vagy AI Provider Privacy & Vendor Register keretében tarthatja nyilván.

9.10. Production AI Privacy Baseline

Az Axion production környezetében AI-szolgáltató vagy konfiguráció csak akkor használható olyan processingre, amely személyes adatot érint, ha az Axion az adott use case szempontjából megfelelően értékelte a releváns adatvédelmi és biztonsági feltételeket.

Az értékelés körébe tartozhat különösen az adatfelhasználás célja, model training és service improvement feltételei, retention, provider-side hozzáférés, security és abuse monitoring, adatkezelési régió, nemzetközi adattovábbítás, DPA vagy más szerződéses feltételek, al-adatfeldolgozók és az adott adatkategóriára vonatkozó korlátozások.

A Privacy Policy nem helyettesíti ezt a provider-szintű ellenőrzést: konkrét „no training”, Zero Data Retention, retention duration, regional processing vagy hasonló garancia csak akkor kommunikálható a Felhasználók felé, ha azt az alkalmazott production szolgáltatás ténylegesen biztosítja.

10. Adatbiztonság és személyesadat-incidensek

10.1. Általános adatbiztonsági elvek

Az Axion a személyes adatok védelme érdekében a kockázatokhoz igazodó technikai és szervezési intézkedéseket alkalmaz. Ezen intézkedések célja különösen a személyes adatok bizalmasságának, sértetlenségének és rendelkezésre állásának védelme, valamint a jogosulatlan hozzáférés, közlés, módosítás, elvesztés vagy megsemmisülés kockázatának csökkentése.

A megfelelő biztonsági szint meghatározásakor az Axion figyelembe veszi különösen az adatkezelés jellegét, hatókörét, körülményeit és céljait, az érintett személyes adatok jellegét, valamint a természetes személyek jogaira és szabadságaira jelentett kockázatokat.

Az Axion biztonsági intézkedéseit a technológia, a szolgáltatás és a kockázati környezet változásával összhangban felülvizsgálhatja és fejlesztheti.

10.2. Infrastruktúra, adatátvitel és tárolás védelme

Az Axion megfelelő védelmi intézkedéseket alkalmazhat a személyes adatok hálózati továbbítása, infrastruktúrán belüli feldolgozása és tárolása során, ideértve az adott rendszerhez és use case-hez megfelelő titkosítási, hozzáférés-védelmi, hálózati, konfigurációs és infrastruktúra-biztonsági kontrollokat.

A konkrét technikai megoldások az érintett Axion-komponenstől, infrastruktúrától, adattípustól és szolgáltatói környezettől függhetnek, és biztonsági okból nem minden implementációs részlet nyilvános.

A külső infrastruktúra- és technológiai szolgáltatókra a 4., 5. és 9. fejezet további szabályai irányadók.

10.3. Credentialök, secretek és Connected Service tokenek

Az Axion a jelszavakat, API-kulcsokat, access és refresh tokeneket, secreteket és más hitelesítési vagy authorization adatokat biztonsági szempontból érzékeny információként kezeli.

Az ilyen adatokhoz való hozzáférést az Axion a szükséges személyekre, rendszerekre és műveletekre korlátozza, és megfelelő technikai védelmet alkalmaz a jogosulatlan hozzáférés, kiszivárgás vagy visszaélés kockázatának csökkentésére.

Connected Service tokenek és más authorization adatok kezelésére az adott integrációra vonatkozó szabályok, így különösen a 8. fejezet is irányadó.

10.4. Hozzáférés-kezelés és staff access

Az Axion személyes adataihoz csak olyan felhatalmazott személy vagy rendszer férhet hozzá, amelynek az adott hozzáférésre megfelelő működési, support-, biztonsági, jogi vagy más jogszerű célból szüksége van.

Az Axion a hozzáféréseket a least privilege és need-to-know elvéhez igazítja, és megfelelő jogosultságkezelési, hitelesítési, felülvizsgálati és – ahol indokolt – naplózási kontrollokat alkalmazhat.

Az Axion staff vagy más felhatalmazott személy személyes adathoz való hozzáférése nem jelent általános jogosultságot a Felhasználói tartalom megtekintésére; a hozzáférésnek konkrét és jogszerű célhoz kell kapcsolódnia.

10.5. Account security, confirmation és izolált végrehajtás

Az Axion Account- és session-biztonsági, authentication- és más védelmi mechanizmusokat alkalmazhat a jogosulatlan hozzáférés kockázatának csökkentésére. A Felhasználó felel a saját hozzáférési adatainak megfelelő védelméért és azért, hogy észszerű biztonsági intézkedéseket alkalmazzon az Account használata során.

Ha ugyanahhoz az Accounthoz több személy fér hozzá, az növelheti a jogosulatlan hozzáférés, Connected Service adatok elérése és a műveletek személyhez rendelésének kockázatát.

A külső hatással járó támogatott Actions esetén az Axion confirmationt vagy más Felhasználói jóváhagyást alkalmazhat a nem kívánt műveletek kockázatának csökkentésére.

Kód, workflow vagy más végrehajtható tartalom futtatása esetén az Axion izolált vagy sandboxolt végrehajtási környezetet és más megfelelő biztonsági kontrollokat használhat. Az izoláció csökkenti, de nem szünteti meg teljesen a hibás vagy rosszindulatú kódhoz kapcsolódó kockázatokat.

10.6. Technológiai szolgáltatók és biztonsági kontrollok

Az Axion olyan technológiai szolgáltatókat vehet igénybe, amelyek a saját szolgáltatásukhoz kapcsolódó biztonsági intézkedéseket alkalmaznak. Az Axion a szolgáltatók kiválasztása és használata során az adott processing kockázataihoz igazodva figyelembe veszi a releváns adatvédelmi és biztonsági feltételeket.

Külső szolgáltató alkalmazása nem szünteti meg az Axionra az adott adatkezelési szerepében vonatkozó kötelezettségeket.

A provider governance, al-adatfeldolgozók, nemzetközi adattovábbítások és AI-provider security további szabályait a 4., 5. és 9. fejezet tartalmazza.

10.7. Logging, monitoring, backup és vulnerability management

Az Axion megfelelő logging-, monitoring-, backup-, helyreállítási, hibakezelési és vulnerability management folyamatokat alkalmaz a szolgáltatás biztonságának, rendelkezésre állásának és integritásának támogatására.

A biztonsági naplók és monitoring adatok személyes adatot is tartalmazhatnak; ezek kezelésére a 2., 3. és 6. fejezet szabályai irányadók.

Az Axion a szolgáltatás jellegéhez és kockázataihoz igazodó biztonsági tesztelést, sérülékenység-kezelést és más ellenőrzéseket végezhet. A konkrét tesztelési módszerek, biztonsági architektúra és belső eljárások részletei biztonsági okból nem feltétlenül nyilvánosak.

10.8. Személyesadat-incidensek felismerése és kezelése

Nem minden technikai vagy biztonsági esemény minősül a GDPR szerinti személyesadat-incidensnek.

Személyesadat-incidensnek minősülhet a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

Az Axion a tudomására jutott potenciális személyesadat-incidenst megfelelően megvizsgálja, értékeli annak jellegét, terjedelmét, érintett adatkategóriáit, lehetséges következményeit és az érintettek jogaira és szabadságaira jelentett kockázatot, és szükség szerint intézkedéseket tesz az incidens korlátozására, elhárítására és következményeinek mérséklésére.

10.9. Hatósági és érintetti értesítés

Ha az Axion adatkezelőként olyan személyesadat-incidensről szerez tudomást, amely a GDPR alapján felügyeleti hatósági bejelentést igényel, az Axion azt indokolatlan késedelem nélkül és – ha lehetséges – legkésőbb 72 órával azután jelenti be az illetékes felügyeleti hatóságnak, hogy az incidens a tudomására jutott.

Nem szükséges hatósági bejelentés, ha a személyesadat-incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

Ha a személyesadat-incidens valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve, az Axion az alkalmazandó GDPR-szabályok szerint indokolatlan késedelem nélkül tájékoztatja az érintetteket, kivéve, ha valamely jogszabályi kivétel alkalmazható.

A security event ténye önmagában tehát nem jelenti automatikusan, hogy hatósági vagy érintetti notification szükséges; ezt az incidens jogi és kockázati értékelése határozza meg.

10.10. Incidensdokumentáció és processor-helyzetek

Az Axion a személyesadat-incidenseket a GDPR által megkövetelt módon dokumentálja, ideértve szükség szerint az incidens körülményeit, hatásait és a megtett korrekciós intézkedéseket.

Ha az Axion valamely processing tekintetében adatfeldolgozóként jár el, az Axion a személyesadat-incidensről való tudomásszerzést követően indokolatlan késedelem nélkül értesíti az érintett adatkezelőt, és az alkalmazandó DPA, dokumentált utasítások és jogszabályok szerint együttműködik az incidens kezelésében.

Ha az incidens az Axion valamely adatfeldolgozójánál vagy al-adatfeldolgozójánál következik be, az Axion a saját adatkezelési szerepe és az alkalmazandó szerződéses, illetve jogi kötelezettségei szerint értékeli és kezeli a helyzetet.

10.11. Security incident bejelentése és a biztonság korlátai

A Felhasználó vagy más személy az Axionnal kapcsolatos feltételezett adatvédelmi vagy biztonsági problémát a support@axionaiapp.com e-mail-címen jelezheti, ideértve azt az esetet is, amikor az Accountjához nem tud hozzáférni.

Az Axion és technológiai szolgáltatói megfelelő biztonsági intézkedések alkalmazására törekednek, azonban egyetlen internetes, felhőalapú vagy AI-szolgáltatás sem garantálhat abszolút biztonságot vagy azt, hogy biztonsági esemény soha nem következik be.

Külső támadás, harmadik személy jogellenes cselekménye vagy más security event ténye önmagában nem határozza meg az Axion jogi felelősségét. Az Axion felelősségét az alkalmazandó jog, az incidens konkrét körülményei, az Axion adatkezelési szerepe és az alkalmazott technikai és szervezési intézkedések megfelelősége alapján kell megítélni.

10.12. Privacy by Design, felülvizsgálat és DPIA

Az Axion a személyes adatok kezelését érintő új vagy lényegesen módosított funkciók, rendszerek és processingek kialakításakor a Privacy by Design és Privacy by Default elveit figyelembe veszi, és az adatvédelmi követelményeket a technikai és terméktervezési döntésekbe a kockázatokhoz igazodva beépíti.

Az Axion a releváns adatvédelmi és biztonsági kockázatokat, hozzáféréseket, szolgáltatói függőségeket és védelmi intézkedéseket megfelelő időközönként, illetve lényeges változás esetén felülvizsgálhatja.

Ha egy tervezett adatkezelés a GDPR alapján valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az Axion az adatkezelés megkezdése előtt adatvédelmi hatásvizsgálatot (Data Protection Impact Assessment, DPIA) végez, amennyiben azt az alkalmazandó jog megköveteli.

A részletes Information Security Policy, Incident Response Plan, Access Control Policy, Vulnerability Management Procedure és más belső security dokumentáció nem képezi jelen publikus Tájékoztató részét.

11. Cookie-k, analitika és hasonló technológiák

11.1. Cookie-k és hasonló technológiák

Az Axion webes felülete cookie-kat, local storage-ot és más hasonló technológiákat használhat a szolgáltatás működtetéséhez, biztonságához, a Felhasználó beállításainak megőrzéséhez, valamint – megfelelő jogalap és szükség esetén hozzájárulás mellett – analitikai célokra.

E technológiák segítségével az Axion vagy az általa igénybe vett szolgáltató információt tárolhat a Felhasználó eszközén, illetve hozzáférhet az ott tárolt információhoz. Az alkalmazandó adatvédelmi és elektronikus hírközlési szabályokat az Axion az adott technológia célja és működése szerint alkalmazza.

11.2. Feltétlenül szükséges technológiák

Az Axion olyan cookie-kat vagy hasonló technológiákat használhat, amelyek a Felhasználó által kifejezetten igénybe vett szolgáltatás biztosításához vagy a szolgáltatás biztonságos működéséhez feltétlenül szükségesek.

Ide tartozhatnak különösen az authentication- és session-kezeléshez, biztonsághoz, fraud- vagy abuse-preventionhöz, terheléselosztáshoz, alapvető felhasználói beállításokhoz, valamint a cookie- vagy privacy-preferencia megjegyzéséhez szükséges technológiák.

Ha az alkalmazandó jog szerint az ilyen technológiák használatához nem szükséges hozzájárulás, az Axion azokat a szolgáltatás működéséhez szükséges körben hozzájárulás nélkül alkalmazhatja. Ezek nem használhatók pusztán opcionális analitikai vagy marketing cél elrejtésére.

11.3. Analitika és PostHog

Az Axion PostHogot használhat webes és termékanalitikai célokra annak megértéséhez, hogy a Felhasználók hogyan használják a szolgáltatást, mely funkciók működnek megfelelően, hol jelentkeznek hibák vagy teljesítményproblémák, és hogyan fejleszthető a felhasználói élmény.

Az analitikai adatok tartalmazhatnak például esemény- és funkcióhasználati adatokat, oldal- vagy képernyőinterakciókat, technikai eszköz- és böngészőinformációkat, időbélyegeket, pseudonymous identifiereket, valamint az adott konfigurációtól függő hálózati vagy account-kapcsolati metaadatokat.

Az opcionális PostHog- vagy más analitikai funkciók használata az alkalmazandó consent- és adatvédelmi követelményekhez igazodik.

11.4. Analitikai adatminimalizálás és tartalmi korlátozások

Az Axion analitikai rendszerének célja nem a Chat-, Input-, Output-, dokumentum-, Connected Service- vagy más Felhasználói tartalom teljes szövegének általános begyűjtése analitikai célból.

Az Axion az analytics konfiguráció során arra törekszik, hogy a szolgáltatás fejlesztéséhez szükséges esemény- és technikai adatokat használja, és megfelelő masking-, suppression-, exclusion- vagy más adatminimalizálási kontrollokat alkalmazzon, ha egy analitikai funkció érzékeny mezőt vagy tartalmat érinthet.

Credentialök, jelszavak, secretek, authorization tokenek és más hitelesítési adatok nem használhatók rendeltetésszerű analitikai tartalomként.

11.5. Hozzájárulás és consent gating

Ha az opcionális analitikai cookie vagy hasonló technológia használatához az alkalmazandó jog szerint előzetes hozzájárulás szükséges, az Axion az ilyen technológiát csak megfelelő hozzájárulás után aktiválja.

A Felhasználó számára valódi választási lehetőséget kell biztosítani az opcionális technológiák elfogadása és elutasítása között. Az opcionális analytics elutasítása önmagában nem akadályozhatja az Axion azon alapvető funkcióinak használatát, amelyekhez az ilyen analitika nem szükséges.

A hozzájárulásnak önkéntesnek, megfelelően tájékozottnak, konkrétnak és egyértelműnek kell lennie, ahol az alkalmazandó jog ezt megköveteli. Az Axion nem tekinti az oldal puszta használatát vagy továbbgörgetését automatikusan opcionális analitikai hozzájárulásnak.

11.6. Consent módosítása és visszavonása

A Felhasználó az Axion által biztosított cookie- vagy privacy-beállításokon keresztül módosíthatja vagy visszavonhatja az opcionális technológiákhoz adott hozzájárulását, ha ilyen technológiák használatban vannak.

A hozzájárulás visszavonásának olyan egyszerűnek kell lennie, mint annak megadása. A visszavonás nem érinti a visszavonás előtt jogszerűen végzett adatkezelést.

Az Axion a consent state-et és a hozzájárulás kezeléséhez szükséges bizonyítékokat megfelelő ideig dokumentálhatja annak igazolására, hogy az adott preferenciát tiszteletben tartotta.

11.7. Session Replay, autocapture és fejlettebb analitikai funkciók

Az Axion csak megfelelő adatvédelmi értékelés mellett használhat Session Replayt, autocapture-t vagy más olyan fejlett analitikai funkciót, amely a hagyományos eseménymérésnél részletesebb felhasználói interakciót rögzíthet.

Ha ilyen funkció használatban van, az Axion megfelelő masking-, input suppression-, route exclusion-, hozzáférés-korlátozási és retention-beállításokat alkalmaz, és ahol az alkalmazandó jog ezt megköveteli, a funkciót csak előzetes hozzájárulás után aktiválja.

Az Axionnak különösen figyelembe kell vennie, hogy a szolgáltatás Chatet, dokumentumokat, üzleti információkat, Connected Service adatokat és más érzékeny tartalmat kezelhet, ezért az ilyen adatok indokolatlan rögzítése fejlett analytics funkcióval kerülendő.

11.8. Analytics identifier, IP-cím és pseudonymous adatok

Az analitikai rendszerek pseudonymous vagy más technikai identifiert használhatnak az események, sessionök vagy eszközök összekapcsolására. Bejelentkezett Felhasználó esetén egyes analitikai események az Accounttal is összekapcsolhatók, ha ez a meghatározott analitikai célhoz szükséges és jogszerű.

A pseudonymizált vagy technikai identifier továbbra is személyes adatnak minősülhet, ha természetes személyhez közvetlenül vagy közvetve kapcsolható.

IP-cím vagy abból származó helymeghatározási információ kezelése az adott analytics és infrastruktúra konfigurációjától függhet. Az Axion arra törekszik, hogy az ilyen adatot csak a szükséges körben kezelje, és ahol megfelelő, csökkentett pontosságú, rövid ideig megőrzött vagy más módon minimalizált megoldást alkalmazzon.

11.9. Megőrzés, aggregálás és marketing tracking

Az analitikai személyes adatok megőrzési idejét az Axion az analitikai célhoz, az alkalmazott szolgáltatás konfigurációjához és a 6. fejezet megőrzési elveihez igazítja. Az Axion törekedhet arra, hogy ahol a cél elérhető, személyhez nem kapcsolható aggregált vagy anonimizált statisztikákat használjon.

Az Axion jelenlegi termékanalitikai célú technológiáinak használata önmagában nem jelenti harmadik fél által végzett behavioural advertising vagy advertising profiling alkalmazását.

Ha az Axion a jövőben marketing-, advertising-, retargeting- vagy más, a jelenlegi termékanalitikától lényegesen eltérő tracking technológiát vezet be, annak alkalmazását külön megfelelő jogalaphoz és – ahol szükséges – consenthez köti, és a Felhasználókat megfelelően tájékoztatja.

11.10. Cookie Policy, user controls és compliance

Jelen Tájékoztató a cookie-k és hasonló technológiák használatának adatvédelmi alapelveit tartalmazza. Az Axion külön Cookie Policyban vagy Cookie Notice-ban adhat részletes, aktuális tájékoztatást az alkalmazott technológiákról, ideértve különösen azok nevét,

providerét, célját, kategóriáját, időtartamát, first-party vagy third-party jellegét és consent státuszát.

A böngésző vagy eszköz által küldött Do Not Track, Global Privacy Control vagy más privacy preference signal kezelését az Axion az alkalmazandó jog, a tényleges technikai implementáció és az adott signal követelményei szerint határozza meg. Az Axion nem állítja, hogy valamely ilyen signal támogatott, amíg azt ténylegesen nem implementálta és ellenőrizte.

12. Kiskorúak, különleges adatok és harmadik személyek adatai

12.1. 18 éven felülieknek szánt szolgáltatás

Az Axion szolgáltatását kizárólag 18. életévüket betöltött személyek használhatják. Az Axion Account létrehozásával és a szolgáltatás használatával a Felhasználó kijelenti, hogy megfelel az alkalmazandó korhatári követelménynek.

Ha az Axion megalapozottan tudomást szerez arról, hogy egy Accountot a szolgáltatásra vonatkozó korhatárt el nem érő személy használ, az Axion megfelelő intézkedést tehet, ideértve az Account hozzáférésének korlátozását vagy megszüntetését és a kapcsolódó adatok kezelésének felülvizsgálatát.

A korhatár a szolgáltatás Felhasználójára vonatkozik, és nem jelenti azt, hogy az Axionon keresztül feldolgozott tartalom kizárólag nagykorú személyek adatait tartalmazhatja.

12.2. Kiskorúak adatai a Felhasználói tartalomban

A Felhasználó által megadott Input, feltöltött dokumentum, Connected Service adat, webes kutatás eredménye, User-operated application vagy más tartalom 18 év alatti érintettre vonatkozó személyes adatot is tartalmazhat.

Az ilyen adat feldolgozása nem jelenti azt, hogy a kiskorú maga az Axion Felhasználója. A gyermekekre vonatkozó személyes adatok azonban az adatkezelés körülményeitől függően fokozott védelmet és különös adatvédelmi figyelmet igényelhetnek.

A Felhasználó felel azért, hogy az általa az Axion rendelkezésére bocsátott gyermekadatok kezeléséhez megfelelő jogalappal, jogosultsággal és – ahol szükséges – megfelelő tájékoztatási vagy hozzájárulási mechanizmussal rendelkezzen, ha az adott processing tekintetében ő az adatkezelő.

12.3. Különleges személyes adatok

Az Axion általános használatához főszabály szerint nincs szükség a GDPR 9. cikke szerinti különleges személyes adatok megadására.

A Felhasználó által biztosított Input, dokumentum, Connected Service adat vagy más tartalom azonban tartalmazhat például faji vagy etnikai származásra, politikai véleményre, vallási vagy

világnézeti meggyőződésre, szakszervezeti tagságra, genetikai vagy biometrikus adatra, egészségügyi adatra, illetve szexuális életre vagy szexuális irányultságra vonatkozó személyes adatot.

Ha ilyen adat a Felhasználó által kért feladat részét képezi, az az adott processing keretében AI-, dokumentum-, keresési, tárolási vagy más szükséges technikai feldolgozásba kerülhet a jelen Tájékoztatóban leírt adatáramlások szerint.

12.4. Különleges adatok jogalapja és büntetőjogi adatok

Különleges személyes adat kezelése csak akkor jogszerű, ha a GDPR 6. cikke szerinti megfelelő jogalap mellett a GDPR 9. cikkében meghatározott megfelelő feltétel is fennáll. Ez az adott processing körülményeitől függően lehet például kifejezett hozzájárulás vagy más, jogszabályban meghatározott kivétel.

Az Axion nem tekinti automatikusan valamennyi, Felhasználó által megadott különleges személyes adat kezelését kifejezett hozzájáruláson alapulónak; a megfelelő jogalapot és 9. cikk szerinti feltételt az adott adatkezelési szerep és processing alapján kell meghatározni.

A büntetőjogi felelősség megállapítására és bűncselekményekre vonatkozó személyes adatok nem a GDPR 9. cikke szerinti különleges adatkategóriák közé tartoznak, hanem a GDPR 10. cikke szerinti külön szabályozás alá esnek. Ilyen adat kezelése csak az alkalmazandó jog által megengedett keretek között történhet.

12.5. Harmadik személyek személyes adatai

Az Axionba bevitt vagy az Axionon keresztül feldolgozott tartalom a Felhasználón kívüli más természetes személy személyes adatát is tartalmazhatja.

Ha a Felhasználó más személy személyes adatát adja át az Axionnak, a Felhasználó felel azért, hogy erre megfelelő jogosultsággal és – amennyiben ő az adatkezelő – megfelelő adatvédelmi jogalappal rendelkezzen, valamint teljesítse az őt terhelő tájékoztatási és más adatkezelői kötelezettségeket.

Az Axion nem képes és nem köteles minden egyes Felhasználói Input vagy feltöltött dokumentum esetében előzetesen ellenőrizni a Felhasználó adatkezelési jogalapját. Ez nem érinti az Axion saját adatkezelési szerepében fennálló kötelezettségeit.

12.6. Nyilvános források és webes kutatás

Az Axion webes keresési vagy kutatási funkciói nyilvánosan elérhető forrásból személyes adatot is feldolgozhatnak.

Az, hogy valamely személyes adat nyilvánosan hozzáférhető, önmagában nem jelenti azt, hogy az adat korlátozás nélkül, bármely célra felhasználható. Az ilyen adat kezelésére továbbra is az alkalmazandó adatvédelmi, személyiségi jogi és más jogszabályok vonatkozhatnak.

A webes keresés vagy kutatás használata önmagában nem jelenti azt, hogy az Axion az érintettekről általános vagy tartós profilalkotást végez. Ha egy konkrét processing

profilalkotásnak vagy más külön szabályozott adatkezelésnek minősül, arra az alkalmazandó jog további követelményei irányadók.

12.7. AI által generált vagy kikövetkeztetett személyes adatok

Az AI-modellek személyre vonatkozó állításokat, összefoglalásokat, értékeléseket, következtetéseket vagy más inference-eket hozhatnak létre a rendelkezésükre bocsátott adatok alapján.

Az AI által generált személyes állítás nem tekinthető automatikusan ellenőrzött ténynek. Az AI Output pontatlan, hiányos, elavult vagy téves információt, illetve megalapozatlan következtetést is tartalmazhat.

Ha az AI Output természetes személyre vonatkozó személyes adatnak minősül, annak további felhasználása során az alkalmazandó adatvédelmi követelményeket figyelembe kell venni. Különösen érzékeny vagy jelentős következménnyel járó személyi állítás esetén megfelelő emberi ellenőrzés lehet szükséges.

12.8. Magas jelentőségű személyi döntések

Az Axion által létrehozott AI Output nem kezelhető automatikusan hiteles vagy kizárólagos alapként olyan döntéshez, amely természetes személy jogaira, lehetőségeire vagy életkörülményeire jelentős hatással lehet.

Különös körültekintés szükséges például foglalkoztatási, hitel- vagy biztosítási, egészségügyi, oktatási, lakhatási, jogi, hatósági vagy más magas jelentőségű személyi döntések esetén.

A Felhasználó felel azért, hogy az ilyen Output felhasználása során biztosítsa az adott use case-re alkalmazandó jogi követelményeket, megfelelő emberi felülvizsgálatot és szükséges szakmai ellenőrzést. A kizárólag automatizált döntéshozatalra vonatkozó GDPR-szabályokat a 7.9. pont ismerteti.

12.9. Harmadik személyek adatainak provider-feldolgozása

Ha a Felhasználói Input, dokumentum, Connected Service adat vagy más tartalom harmadik személy személyes adatát tartalmazza, az adat a Felhasználó által kért feladat teljesítéséhez szükséges mértékben az Axion megfelelő technológiai szolgáltatóihoz, ideértve AI-szolgáltatókat is, továbbításra kerülhet.

Az orchestration nem jelenti azt, hogy az ilyen adat automatikusan valamennyi AI-providerhez vagy más szolgáltatóhoz eljut. Az adatáramlás az adott feladat, routing, toolhasználat és szükséges processing alapján történik.

A szolgáltatók, al-adatfeldolgozók, nemzetközi adattovábbítások és AI-routing további szabályait a 4., 5. és 9. fejezet tartalmazza.

12.10. Tájékoztatási kötelezettségek és érintetti jogok

Ha az Axion valamely személyes adat tekintetében adatkezelőként jár el, az Axion felel az őt terhelő adatkezelői tájékoztatási és érintetti jogi kötelezettségek teljesítéséért.

Ha a Felhasználó valamely User-operated processing tekintetében adatkezelő, és az Axion kizárólag adatfeldolgozóként jár el, a GDPR 13. vagy 14. cikke szerinti tájékoztatás és az érintetti kérelmek elsődleges kezelése főszabály szerint a Felhasználó adatkezelői felelőssége. Az Axion az alkalmazandó DPA, dokumentált utasítások és GDPR-követelmények szerint segítséget nyújt.

Az érintetti jogok Axion általi kezelésének általános szabályait a 7. fejezet tartalmazza.

12.11. User-operated applications és gyermekeket vagy érzékeny adatot érintő use case-ek

A Felhasználó az Axion segítségével olyan User-operated applicationt, workflow-t vagy más megoldást hozhat létre vagy működtethet, amely gyermekek személyes adatait, különleges személyes adatokat, büntetőjogi adatokat vagy más érzékeny információt kezel.

Az ilyen alkalmazás létrehozása vagy Axion-infrastruktúrán történő támogatása önmagában nem teszi az Axiont az adott User-operated processing adatkezelőjévé. Ha a processing céljait és lényeges eszközeit a Felhasználó határozza meg, a Felhasználó lehet az adatkezelő, az Axion pedig az adott processing tekintetében adatfeldolgozóként járhat el.

A User-operated application üzemeltetője felel az alkalmazására vonatkozó korhatári, gyermekvédelmi, privacy notice-, jogalapi, consent-, age-assurance-, különlegesadat-kezelési és más alkalmazandó követelmények meghatározásáért és teljesítéséért. Az Axion saját adatfeldolgozói kötelezettségei ettől függetlenül fennmaradnak.

Az adatkezelő–adatfeldolgozó szerepek és a User-operated processing részletes szabályait a 13. fejezet tartalmazza.

12.12. Adatminimalizálás és felelős használat

A Felhasználónak törekednie kell arra, hogy a feladat teljesítéséhez szükségesnél több személyes adatot ne adjon meg az Axionnak, különösen akkor, ha a feladat érzékeny vagy harmadik személyekre vonatkozó információt érint.

Indokolatlanul kerülendő különösen gyermekek személyes adatainak, egészségügyi, genetikai vagy biometrikus adatoknak, büntetőjogi adatoknak, pénzügyi azonosítóknak, credentialöknek, secreteknek, illetve más személyek érzékeny információinak megadása, ha azok a feladat teljesítéséhez nem szükségesek.

Magas kockázatú processing esetén az Axion és – User-operated processingnél – az adatkezelő Felhasználó köteles lehet további adatvédelmi értékelést vagy DPIA-t végezni, ha azt a GDPR megköveteli. Az Axion saját Privacy by Design és DPIA elveit a 10.12. pont tartalmazza.

A részletes high-risk processing, special-category és DPIA ellenőrzési eljárások belső compliance dokumentációban tarthatók fenn.

13. Adatkezelői és adatfeldolgozói szerepek, User-operated processing

13.1. Az adatvédelmi szerepek funkcionális meghatározása

Az Axion adatvédelmi szerepét minden esetben az adott adatkezelési művelet tényleges körülményei alapján kell meghatározni. Egyes processingek tekintetében az Axion adatkezelőként, más processingek tekintetében adatfeldolgozóként járhat el.

A szerep meghatározásánál különösen azt kell vizsgálni, hogy ki határozza meg a személyes adatok kezelésének céljait és lényeges eszközeit, illetve hogy az Axion saját célból vagy egy másik adatkezelő dokumentált utasításai alapján végzi-e a processinget.

Ugyanazon Felhasználói vagy üzleti kapcsolatban ezért több, egymástól eltérő adatvédelmi szerep párhuzamosan is fennállhat.

13.2. Amikor az Axion adatkezelő

Az Axion adatkezelőként járhat el különösen azoknál a processingeknél, amelyek célját és lényeges eszközeit saját maga határozza meg a saját szolgáltatásának működtetéséhez.

Ide tartozhat különösen az Account létrehozása és kezelése, authentication, billing és AEC- vagy más szolgáltatási tranzakciók kezelése, security és fraud/abuse prevention, support, jogi és compliance kötelezettségek teljesítése, valamint az Axion saját szolgáltatásának szükséges működési és analitikai adatkezelése.

Az Axion ilyen processingek tekintetében maga felel az alkalmazandó adatkezelői kötelezettségek teljesítéséért. Az ezekhez igénybe vett technológiai szolgáltatók szerepe az adott szolgáltatástól és szerződéses konstrukciótól függően adatfeldolgozói, al-adatfeldolgozói vagy más önálló adatkezelői szerep lehet.

13.3. User-operated processing és a Felhasználó adatkezelői szerepe

Ha a Felhasználó az Axion segítségével olyan alkalmazást, workflow-t, automatizmust vagy más megoldást hoz létre vagy üzemeltet, amelyben a személyes adatok kezelésének céljait és lényeges eszközeit a Felhasználó határozza meg, a Felhasználó az adott processing tekintetében adatkezelőként járhat el.

Ilyen döntés lehet különösen annak meghatározása, hogy milyen személyes adatot gyűjt az alkalmazás, kik az érintettek, milyen célból történik az adatkezelés, milyen funkciók használják az adatot, kinek kerül továbbításra, mennyi ideig szükséges megőrizni, illetve milyen Felhasználó által választott integráció vagy harmadik fél szolgáltatás vesz részt a processingben.

Ha a Felhasználó adatkezelő, ő felel különösen a processing jogszerű céljáért és jogalapjáért, az érintettek megfelelő tájékoztatásáért, az alkalmazásszintű adatminimalizálásért, a szükséges hozzájárulásokért vagy más jogalapi feltételekért, valamint az általa meghatározott adatkezelési konfiguráció jogszerűségéért.

13.4. Az Axion mint adatfeldolgozó

Ha az Axion személyes adatot a Felhasználó által meghatározott célból, a Felhasználó nevében és annak dokumentált utasításai alapján dolgoz fel, az Axion az adott processing tekintetében adatfeldolgozóként járhat el.

Ilyen esetben az Axion a rá alkalmazandó GDPR 28. cikk szerinti kötelezettségeket teljesíti, ideértve különösen a dokumentált utasítások szerinti processinget, a megfelelő titoktartási és biztonsági követelményeket, az al-adatfeldolgozók megfelelő kezelését, valamint az adatkezelő részére nyújtandó, jogszabályban előírt segítséget.

Az, hogy az Axion infrastruktúrát, AI-funkciót, kódgenerálást, orchestrationt, tárhelyet vagy más technikai eszközt biztosít egy User-operated application vagy workflow működéséhez, önmagában nem teszi az Axiont az adott User-operated processing adatkezelőjévé.

Ez az elhatárolás nem mentesíti az Axiont az adatfeldolgozóként rá vonatkozó kötelezettségek, illetve az Axion által saját célra végzett adatkezelésekért fennálló adatkezelői kötelezettségek alól.

13.5. User módosításai és User-generated code

A Felhasználó az Axion által létrehozott vagy támogatott alkalmazást, workflow-t vagy kódot módosíthatja, kiegészítheti vagy más rendszerrel integrálhatja. Ilyen módosítás lehet például új adatmező, tracking technológia, külső SDK, adatbázis, API, integráció vagy más adatkezelési funkció hozzáadása.

A Felhasználó által önállóan meghatározott vagy végrehajtott módosítás adatvédelmi következményei nem tulajdoníthatók automatikusan az Axionnak. Ha a módosítás eredményeként új adatkezelési cél, adattípus, címzett vagy technológiai szolgáltató jelenik meg, annak jogszerűségét az adott processing adatkezelőjének kell értékelnie.

Ha az Axion a módosított megoldás bizonyos személyes adatait továbbra is a Felhasználó nevében dolgozza fel, az Axion ezen processing tekintetében fennálló adatfeldolgozói kötelezettségei változatlanul alkalmazandók.

13.6. Dokumentált utasítások, Customer Data és Axion Service Data

Adatfeldolgozói szerepben az Axion a Customer Data-t a Felhasználó dokumentált utasításai, az alkalmazandó Data Processing Agreement vagy Data Processing Terms, valamint a jogszabályok szerint kezeli.

Customer Data lehet különösen a User-operated application vagy workflow végfelhasználóira, ügyfeleire, munkavállalóira vagy más érintettjeire vonatkozó olyan személyes adat, amelyet az Axion a Felhasználó nevében dolgoz fel.

Ettől elkülönülhetnek az Axion Service Data körébe tartozó olyan adatok, amelyeket az Axion saját célból kezel, például Account-, billing-, security-, fraud prevention-, support- vagy szükséges működési metaadatok. Az ilyen adatok tekintetében az Axion adatkezelői szerepe

fennállhat akkor is, ha ugyanazon üzleti kapcsolat más processingjeiben adatfeldolgozóként jár el.

Ha az Axion megítélése szerint valamely dokumentált utasítás sérti az alkalmazandó adatvédelmi jogot, az Axion a jogszabály és az alkalmazandó DPA szerint tájékoztathatja az adatkezelőt, illetve a jog által megengedett vagy megkövetelt módon kezelheti az utasítást.

13.7. Al-adatfeldolgozók

Ha az Axion adatfeldolgozóként jár el, a Customer Data processingjéhez megfelelő al-adatfeldolgozókat vehet igénybe az alkalmazandó Data Processing Agreement vagy Data Processing Terms szerint.

Az Axion által használt infrastruktúra-, AI-, sandbox-, média-, dokumentumfeldolgozási vagy más technológiai szolgáltató akkor minősülhet al-adatfeldolgozónak, amikor Customer Data-t az Axion nevében, az adatfeldolgozói lánc részeként kezel. A szolgáltató szerepét ezért az adott processing és szerződéses konstrukció alapján kell meghatározni.

A Microsoft Azure például az Axion infrastruktúrájának fontos szolgáltatója, és olyan processing esetén, ahol Customer Data-t az Axion adatfeldolgozói szolgáltatásának részeként kezel, al-adatfeldolgozói szerepet tölthet be. Hasonló elv alkalmazandó más technológiai providerekre is.

Az aktuális al-adatfeldolgozói kör, a kapcsolódó szolgáltatások és – ahol releváns – processing helyszínek külön Subprocessor List vagy Register keretében tarthatók naprakészen.

13.8. Processor security, confidentiality és incidensek

Adatfeldolgozói szerepben az Axion megfelelő technikai és szervezési intézkedéseket alkalmaz a Customer Data védelmére, és biztosítja, hogy a személyes adatok kezelésére feljogosított személyek megfelelő titoktartási kötelezettség alatt álljanak vagy megfelelő jogszabályi titoktartási kötelezettség vonatkozzon rájuk.

Ha az Axion adatfeldolgozóként olyan személyesadat-incidensről szerez tudomást, amely az adatkezelő Customer Data-ját érinti, az Axion indokolatlan késedelem nélkül értesíti az érintett adatkezelőt, és az alkalmazandó DPA és jogszabályok szerint együttműködik az incidens kezelésében.

Az általános adatbiztonsági és incidenskezelési elveket a 10. fejezet tartalmazza.

13.9. Érintetti jogok, DPIA és compliance assistance

Ha a Felhasználó a User-operated processing adatkezelője, az érintetti kérelmek elsődleges kezelése a Felhasználó feladata. Az Axion a processing jellegét figyelembe véve és a rendelkezésére álló információk, illetve technikai lehetőségek keretében megfelelő segítséget nyújt az adatkezelőnek a GDPR szerinti érintetti jogok teljesítésében, amennyiben erre adatfeldolgozóként köteles.

Az Axion az alkalmazandó jog és DPA szerint megfelelő segítséget nyújthat az adatkezelőnek az adatbiztonsági kötelezettségek, személyesadat-incidensek, adatvédelmi hatásvizsgálatok és – ahol szükséges – előzetes hatósági konzultáció teljesítéséhez.

Az ilyen segítség nem ruházza át az adatkezelőre tartozó döntéseket az Axionra, és nem változtatja meg automatikusan a felek adatvédelmi szerepét.

13.10. Nemzetközi adattovábbítás, törlés és visszaadás

Ha az Axion adatfeldolgozói szolgáltatásának részeként Customer Data az Európai Gazdasági Térségen kívülre kerül továbbításra vagy ott hozzáférhetővé válik, az Axion az alkalmazandó nemzetközi adattovábbítási követelményeket és a DPA-ban meghatározott megfelelő garanciákat alkalmazza. A nemzetközi adattovábbítás általános szabályait az 5. fejezet tartalmazza.

Az adatfeldolgozói szolgáltatás megszűnésekor vagy az adatkezelő megfelelő utasítására az Axion a DPA és az alkalmazandó jog szerint törli vagy visszaadja a Customer Data-t, kivéve, ha uniós vagy tagállami jog további megőrzést ír elő.

Backupokból, redundáns rendszerekből vagy technikai helyreállítási környezetekből történő végleges eltávolítás kontrollált késleltetéssel történhet, feltéve, hogy az adat addig elkülönített, védett és rendes üzleti processingre nem kerül vissza.

13.11. Data Processing Agreement

Jelen Privacy Policy az Axion adatkezelői és adatfeldolgozói szerepeinek általános, Felhasználók számára szóló magyarázatát tartalmazza, de nem helyettesíti a GDPR 28. cikke szerinti adatfeldolgozói szerződést.

Ha az Axion valamely processing tekintetében adatfeldolgozóként jár el, az adott processingre az Axion Data Processing Agreement vagy Data Processing Terms is alkalmazandó lehet, amely részletesen meghatározza különösen az adatfeldolgozás tárgyát és időtartamát, jellegét és célját, az érintett adatkategóriákat és érintetti csoportokat, az adatkezelő utasításait, a confidentiality és security követelményeket, az al-adatfeldolgozókat, az érintetti jogokhoz és DPIA-hoz nyújtott segítséget, az incidenskezelést, a törlést vagy visszaadást, valamint az alkalmazandó audit- és compliance feltételeket.

A Privacy Policy és a DPA eltérő funkciót tölt be; adatfeldolgozói processing esetén a részletes processor-kötelezettségeket elsősorban az alkalmazandó DPA rendezi.

13.12. Vegyes szerepkörök, joint controllership és felülvizsgálat

Ugyanazon Felhasználói kapcsolatban az Axion különböző processingek tekintetében eltérő adatvédelmi szerepet tölthet be. Az, hogy az Axion egy Customer Data processing tekintetében adatfeldolgozó, nem jelenti azt, hogy saját Account-, billing-, security-, support- vagy más önálló célú processingjei tekintetében is adatfeldolgozó.

Közös adatkezelői (joint controller) kapcsolat nem keletkezik automatikusan pusztán azért, mert az Axion és a Felhasználó ugyanazon technikai rendszerben vagy szolgáltatási láncban

vesz részt. Ha a felek valamely konkrét processing céljait és lényeges eszközeit ténylegesen közösen határozzák meg, az adott processing külön GDPR 26. cikk szerinti értékelést igényelhet.

Az Axion a controller/processor role assessmentet, al-adatfeldolgozói megfelelést és a kapcsolódó DPA-feltételeket a szolgáltatás és a processingek változásával összhangban felülvizsgálhatja.

14. Záró adatvédelmi rendelkezések, átláthatóság és governance

14.1. Átláthatóság és a Privacy Policy elérhetősége

Az Axion a személyes adatok kezeléséről tömör, átlátható, érthető és könnyen hozzáférhető tájékoztatást nyújt. Jelen Privacy Policy az Axion által végzett fő adatkezelési műveletek, adatvédelmi szerepek, címzetti körök, megőrzési elvek és érintetti jogok általános keretét ismerteti.

A Privacy Policy az Axion weboldalán, illetve ahol releváns, az Account létrehozásához, bejelentkezéshez vagy a szolgáltatás használatához kapcsolódó felületeken elérhetővé tehető. Az Axion egyes funkciókhoz vagy processingekhez további, rétegzett vagy kontextuális privacy notice-okat is biztosíthat.

A Privacy Policy megismerése, tudomásulvétele vagy – ahol az alkalmazási folyamat ezt megköveteli – elfogadása önmagában nem minősül valamennyi Axion-adatkezeléshez adott GDPR szerinti hozzájárulásnak. Ha valamely processing hozzájárulást igényel, az Axion azt külön, az alkalmazandó jog követelményeinek megfelelően kéri.

14.2. Az adatkezelő és adatvédelmi kapcsolattartás

Az Axion saját célú adatkezelései tekintetében az adatkezelő az Axion szolgáltatását üzemeltető, jelen Tájékoztatóban vagy a kapcsolódó jogi felületeken megjelölt jogalany.

Adatkezelő: Leiter Miklós Patrik egyéni vállalkozó. Székhely: 4090 Polgár, Hunyadi utca 3. Egyéni vállalkozói nyilvántartási szám: 62674771. Adószám: 92281868-1-29. E-mail: support@axionaiapp.com.

Adatvédelmi, érintetti jogi vagy biztonsági kérdés esetén az Axion a support@axionaiapp.com címen érhető el, ideértve azt az esetet is, amikor az érintett nem rendelkezik Axion Accounttal vagy nem tud ahhoz hozzáférni.

Ha az Axion a jövőben adatvédelmi tisztviselő kijelölésére kötelessé válik, vagy önként adatvédelmi tisztviselőt jelöl ki, annak elérhetőségét az alkalmazandó jog szerint megfelelően közzéteszi.

14.3. Kapcsolódó jogi és adatvédelmi dokumentumok

Jelen Privacy Policy az Axion teljes jogi és adatvédelmi dokumentációjának egyik eleme. A szolgáltatás használatára és egyes processingekre további dokumentumok is alkalmazandók lehetnek, ideértve különösen az Általános Szerződési Feltételeket vagy Terms of Service-t, az Acceptable Use Policyt, a Cookie Policyt vagy Cookie Notice-t, az AI-ra vonatkozó transzparencia-tájékoztatást, a security/trust információkat, valamint adatfeldolgozói processing esetén a Data Processing Agreementet vagy Data Processing Terms-t.

E dokumentumok eltérő funkciót töltenek be. A Privacy Policy elsősorban a személyes adatok kezeléséről és az érintetti jogokról nyújt tájékoztatást; a Terms a szolgáltatási jogviszonyt szabályozza; a Cookie Policy a cookie-k és hasonló technológiák részletes használatát ismerteti; a DPA pedig az adatkezelő és adatfeldolgozó közötti, GDPR 28. cikk szerinti processing feltételeket rendezi.

Ha valamely funkció vagy processing külön tájékoztatást vagy feltételt igényel, az Axion azt a releváns ponton külön is rendelkezésre bocsáthatja.

14.4. A Privacy Policy módosítása

Az Axion időről időre módosíthatja jelen Privacy Policyt, különösen a szolgáltatás, az adatkezelési műveletek, technológiai szolgáltatók, jogszabályok, hatósági gyakorlat, biztonsági követelmények vagy compliance folyamatok változása miatt.

Lényeges adatvédelmi változás esetén az Axion az alkalmazandó jog és a változás jelentősége szerint megfelelő módon tájékoztatja az érintetteket, például a szolgáltatáson belül, a weboldalon, e-mailben vagy más megfelelő csatornán.

A Privacy Policy módosítása önmagában nem hoz létre olyan új adatkezelési jogalapot, amelyhez az alkalmazandó jog szerint külön hozzájárulás, szerződéses alap, érdekmérlegelés vagy más jogalapi feltétel szükséges. Ha egy új vagy módosított processing további jogi feltételt igényel, az Axion azt külön biztosítja.

A Felhasználó számára a mindenkor hatályos Privacy Policy verziója kerül elérhetővé.

14.5. Hatálybalépés, verziók és nyelvi változatok

Jelen Privacy Policy hatálybalépésének és utolsó frissítésének dátumát, valamint – ahol alkalmazott – verziószámát az Axion a dokumentumban vagy annak közzétételi felületén feltünteti.

Az Axion korábbi verziókat jogi, compliance vagy bizonyítási célból megőrizhet, és ahol indokolt, hozzáférhetővé tehet.

A Privacy Policy több nyelven is rendelkezésre állhat. Eltérés vagy értelmezési bizonytalanság esetén, a kötelezően alkalmazandó jog eltérő rendelkezése hiányában, a magyar nyelvű változat az irányadó.

14.6. Felügyeleti hatóság, panasz és bírósági jogorvoslat

Az érintett jogosult adatvédelmi panaszával az Axionhoz fordulni, és jogosult panaszt benyújtani az alkalmazandó GDPR szerint illetékes felügyeleti hatósághoz, különösen a szokásos tartózkodási helye, munkahelye vagy a feltételezett jogsértés helye szerinti tagállamban.

Magyarországon az illetékes felügyeleti hatóság a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH). Cím: 1055 Budapest, Falk Miksa utca 9-11. Levelezési cím: 1363 Budapest, Pf. 9. E-mail: ugyfelszolgalat@naih.hu. Telefon: +36 (1) 391-1400. Honlap: www.naih.hu.

Az Axionhoz történő előzetes panasz vagy kapcsolatfelvétel nem előfeltétele annak, hogy az érintett felügyeleti hatósághoz forduljon vagy az alkalmazandó jog szerint bírósági jogorvoslatot vegyen igénybe.

Az érintetti jogok és jogorvoslatok részletesebb szabályait a 7. fejezet tartalmazza.

14.7. Privacy governance és accountability

Az Axion megfelelő belső adatvédelmi governance és accountability folyamatokat tart fenn annak érdekében, hogy az adatkezelési műveletek megfelelőségét dokumentálja és a szolgáltatás változásával összhangban felülvizsgálja.

A processing jellegétől és az alkalmazandó jogi követelményektől függően ilyen dokumentáció lehet különösen az adatkezelési tevékenységek nyilvántartása (ROPA), adatfeldolgozói nyilvántartás, érdekmérlegelési teszt (LIA), adatvédelmi hatásvizsgálat (DPIA), vendor- és subprocessor review, nemzetközi adattovábbítási értékelés, privacy review, security és incident documentation, valamint más compliance nyilvántartás.

A részletes belső compliance dokumentáció nem képezi szükségszerűen jelen publikus Privacy Policy részét. Az Axion ugyanakkor a GDPR és más alkalmazandó jogszabályok szerint köteles lehet annak megfelelő részeit hatóság vagy más jogosult fél rendelkezésére bocsátani.

14.8. Hatósági és jogérvényesítési megkeresések

Az Axion az illetékes hatóságokkal és bíróságokkal az alkalmazandó jog szerint együttműködik. Személyes adatot hatósági, bírósági vagy más jogérvényesítési megkeresés alapján csak megfelelő jogalap, jogi kötelezettség vagy más alkalmazandó jogi felhatalmazás keretében ad át.

Az Axion a megkeresés jogszerűségét, hatáskörét és terjedelmét az alkalmazandó jog szerint értékelheti, és ahol jogszerű és megfelelő, törekedhet arra, hogy az átadott adat a megkeresés teljesítéséhez szükséges körre korlátozódjon.

Ha az érintett vagy az adatkezelő tájékoztatását jogszabály nem tiltja, az Axion az adott helyzet és jogi kötelezettségei szerint megfelelő tájékoztatást nyújthat.

14.9. Jogutódlás, tényleges processing és jogok elsőbbsége

Az Axion szervezeti átalakulása, jogutódlása, egyesülése, felvásárlása, eszköz- vagy üzletág-átruházása vagy más vállalati tranzakció esetén személyes adatok a tranzakcióhoz szükséges és jogszerű körben átadhatók vagy az adatkezelő személye megváltozhat. Az Axion ilyen esetben az alkalmazandó jog szerinti megfelelő adatvédelmi garanciákat és tájékoztatást biztosítja.

Az Axion jelen Privacy Policyt úgy tartja fenn és frissíti, hogy az megfelelően tükrözze a tényleges adatkezelést. Ha a tényleges processing és a dokumentáció között eltérés kerül azonosításra, az Axion az alkalmazandó jog követelményeinek megfelelően korrigálja a processinget, a dokumentációt vagy mindkettőt.

Jelen Privacy Policy egyetlen rendelkezése sem értelmezhető úgy, hogy korlátozza az érintettet a GDPR vagy más kötelezően alkalmazandó jog alapján megillető jogok gyakorlásában.

14.10. Záró rendelkezések

Ha jelen Privacy Policy valamely rendelkezése részben vagy egészben érvénytelennek, jogellenesnek vagy végrehajthatatlannak bizonyul, ez – amennyiben az alkalmazandó jog ezt lehetővé teszi – nem érinti a többi rendelkezés érvényességét.

A Privacy Policyt az Axion szolgáltatásának tényleges működésével, az alkalmazandó joggal és a kapcsolódó jogi dokumentumokkal együtt kell értelmezni. Eltérés esetén az alkalmazandó kötelező jogszabályok elsőbbséget élveznek.

Utolsó frissítés: 2026. augusztus 17. | Hatálybalépés: 2026. augusztus 17. | Verzió: 1.0