

SOFTWARE LICENSE TERMS

Version **1.2** · Effective Date: **03/09/2026** · Classification: **Public**

Mir.IAM — End User License Agreement (EULA)

Between

Open Products, Networks & Software NV

Operating as “OPNS”

Franklin Rooseveltplaats 12/24

2060 Antwerp, Belgium

VAT BE 0438.031.907

(hereinafter “OPNS” / the “Licensor”)

The Licensee

The entity or individual accepting these terms

(hereinafter the “Licensee”)

OPNS and the Licensee shall jointly be referred to as the “Parties” and individually as a “Party”.

Document type: End User License Agreement

Governing law: Belgium — exclusive jurisdiction of the courts competent for OPNS's registered office

Contents

1. Acceptance, Scope, and Contract Structure.....	2
2. Definitions.....	2
3. Order of Precedence.....	4
4. License Grant.....	5
5. Scope of Use.....	5
6. Product Entitlement, Component Coverage, and License Metrics.....	6
7. License Verification and Excess Use.....	7
8. Affiliates, Authorized Users, and Authorized Resellers.....	7
9. Restrictions.....	8
10. Customer Responsibilities.....	9
11. Customer Environment, Third-Party Systems, and Integrations.....	10
12. Reseller-Supplied Transactions.....	11
13. Support Services.....	12
14. Corrections, Updates, Upgrades, and Supported Versions.....	13
15. End of Life.....	14
16. Customer Data, Usage Data, and Data Protection.....	15
17. Security Responsibilities.....	17
18. Security Incidents, Vulnerability Reports, and Security Testing.....	18
19. No Expansion of Obligations.....	19
20. Intellectual Property, Feedback, and Product Materials.....	19
21. Confidentiality.....	19
22. Third-Party Materials.....	20
23. Warranty Disclaimer.....	20
24. Limitation of Liability.....	21
25. Term, Suspension, and Termination.....	21
26. Export Control, Sanctions, and Legal Compliance.....	22
27. Assignment and Subcontracting.....	23
28. Governing Law, Jurisdiction, and Language.....	23
29. General Legal Terms.....	23
Execution (Optional — Negotiated Signature).....	24
Annex A — Mir.IAM Product Family.....	PGA
Annex B — Trial Use, Evaluation, and Marketplace Distribution.....	PGB

1. Acceptance, Scope, and Contract Structure

These Software License Terms govern Customer's access to and use of the OPNS software products made available under or in connection with the Mir.IAM product family, including applicable software components, Documentation, Corrections, Updates, and other software deliverables made available by OPNS.

The Mir.IAM product family comprises the following Products: **LARA** (Lightweight Access Review Application), **MAYA** (Manage All Your Applications), **PAUL** (Protect & Audit Ubiquitous Libraries), **SARA** (Smart Access Rights Automation), and **ZETI** (Zero Trust Improvements), together with any further software product that OPNS designates in writing as forming part of the Mir.IAM product family. Each of these Products is separately licensed, and these Software License Terms apply to each of them. Annex A identifies the Products forming part of the Mir.IAM product family as at the Effective Date.

By installing, accessing, downloading, deploying, executing, configuring, testing, evaluating, or using the Products, Customer accepts these Software License Terms, unless Customer has entered into a separate written agreement signed by OPNS that expressly supersedes them.

The Products are licensed, not sold. Customer receives only the limited rights expressly granted under these Software License Terms, the applicable Order, and any OPNS-approved product schedule, entitlement record, or component coverage schedule applicable to Customer.

Customer's Product entitlement is determined only by the applicable Order, quote, entitlement record, product schedule, or OPNS-approved component coverage schedule. Product names, bundle names, technical availability, repository access, Documentation, examples, demonstrations, marketing materials, support communications, or prior use do not grant additional rights.

Where the Products are supplied through an Authorized Reseller, Customer's use remains subject to these Software License Terms and to the applicable OPNS-approved Order or entitlement. Authorized Resellers may not grant broader rights, warranties, support commitments, service levels, remedies, or obligations on behalf of OPNS unless OPNS expressly agrees in writing.

These Software License Terms do not make OPNS responsible for the Customer Environment, Third-Party Systems, Authorized Reseller services, customer or reseller configuration, Customer Data quality, testing, access policy decisions, identity governance decisions, or compliance outcomes, except to the limited extent expressly stated in a written agreement signed by OPNS.

2. Definitions

"Affiliate" means any legal entity that directly or indirectly controls, is controlled by, or is under common control with a party, for so long as such control exists.

"Authorized Reseller" means a reseller, distributor, integrator, implementation partner, or other channel partner expressly authorized in writing by OPNS, under a separate agreement with OPNS, to market, resell, distribute, deploy, configure, support, or otherwise make available the Products within the limits of that authorization.

"Authorized User" means an employee, contractor, administrator, technical user, service account, or other individual or non-human user authorized by Customer to access or use the Products solely on Customer's behalf and within the applicable Scope of Use.

"Component" means an individual software element, module, connector, driver, configuration object, policy, script, schema extension, API, interface, workflow extension, monitoring function, governance function, documentation element, or other functional part of a Product.

“Correction” means a patch, bug fix, workaround, minor update, configuration guidance, documentation clarification, or other change made available by OPNS to address a reproducible defect in the Software.

“Customer” means the legal entity that has obtained the right to use the Products directly from OPNS, from an Authorized Reseller, or under an Order that incorporates this EULA.

“Customer Data” means data, content, records, logs, identity data, account data, entitlement data, configuration data, support data, or other information provided by or on behalf of Customer for use with the Products or for related support, maintenance, troubleshooting, or professional services.

“Customer Environment” means the systems, networks, directories, identity sources, applications, databases, infrastructure, cloud environments, third-party platforms, security policies, access policies, configuration settings, operational processes, and data under the control or responsibility of Customer, its Affiliates, its Authorized Users, its Authorized Resellers, or its service providers.

“Documentation” means the technical, functional, operational, administrative, installation, configuration, release, or user documentation made available by OPNS for the Products.

“End Customer” means the final legal entity for whose internal business purposes the Products are licensed or used where the Products are supplied through an Authorized Reseller.

“EULA” means this OPNS / Mir.IAM End User License Agreement, including any terms, schedules, policies, or addenda incorporated by reference into it or into the applicable Order.

“License Metric” means the measurement used to define the permitted scope of use of a Product, including users, managed identities, accounts, objects, systems, applications, connectors, drivers, instances, environments, transactions, authentication events, target systems, servers, tenants, or any other metric stated in the applicable Order, product schedule, entitlement record, or OPNS-approved component coverage schedule.

“Mir.IAM” means the OPNS product family and framework under which the Products are made available, comprising LARA, MAYA, PAUL, SARA, and ZETI and any further Product designated by OPNS as forming part of the Mir.IAM product family, together with the associated framework, Components, blueprint, methodology, and Documentation. A reference to Mir.IAM does not by itself grant any right to Use any individual Product.

“OPNS” means OPNS SA/NV, a company organized under the laws of Belgium, with enterprise number BE0438.031.907, including its affiliates, licensors, successors, and assigns where the context permits.

“Order” means an order form, quote, purchase document, license certificate, statement of entitlement, reseller order, subscription confirmation, product schedule, component coverage schedule, or other written document accepted by OPNS that identifies the Products, quantities, License Metrics, term, fees, support level, Customer, Authorized Reseller, End Customer, and any applicable product-specific terms.

“Personal Data” means any information relating to an identified or identifiable natural person, to the extent protected as personal data, personal information, or an equivalent concept under applicable data protection laws.

“Products” means the OPNS software products, including **LARA, MAYA, PAUL, SARA, and ZETI** and any further software product made available under or in connection with the Mir.IAM product family, together with applicable bundles, modules, Components, Documentation, Updates, Corrections, and related software deliverables made available by OPNS. A reference to a Product includes any successor name, renamed product, or repackaged commercial edition of that Product designated by OPNS in writing.

“Professional Services” means implementation, configuration, integration, consulting, training, migration, analysis, development, customization, project management, or other services provided by OPNS or by an Authorized Reseller, where expressly agreed.

“Regulated Data” means sensitive or regulated information, including health data, payment card data, financial data, biometric data, government identification data, criminal conviction data, special categories of personal data, classified information, or other information subject to specific legal, regulatory, contractual, or sector-specific safeguards.

“Scope of Use” means the permitted usage scope for the Products, including the applicable Products, quantities, License Metrics, territory, Customer entities, Affiliates, environments, deployment model, term, restrictions, and other limits stated in the applicable Order, product schedule, entitlement record, or OPNS-approved component coverage schedule.

“Security Incident” means a confirmed unauthorized access to, alteration of, disclosure of, or compromise of an OPNS-Controlled Environment, Product under OPNS control, or Personal Data processed by OPNS on behalf of Customer.

“Software” means the executable, installable, configurable, or deployable software elements of the Products, including object code, scripts, configuration files, policies, connectors, drivers, libraries, extensions, and any related Updates or Corrections.

“Support Services” means software maintenance, Corrections, Updates, second-line product support, technical assistance, or other support service provided by OPNS where expressly purchased or agreed.

“Third-Party Materials” means open-source software, commercial third-party software, libraries, frameworks, platforms, APIs, tools, dependencies, or other third-party materials included in, distributed with, required by, connected to, or used in combination with the Products.

“Third-Party System” means any system, platform, directory, application, database, API, cloud service, network, operating system, certificate authority, identity source, target system, security tool, or other technology not owned and controlled by OPNS.

“Trial Use” means any evaluation, trial, proof-of-concept, beta, preview, demonstration, free, or pre-release Use of a Product, including any Use obtained through an online marketplace listing, a trial license key issued by OPNS, or any period for which no license fee has been paid. Trial Use is subject to Annex B.

“Update” means a release, maintenance release, minor version, compatibility update, security-related update, documentation update, or technical improvement made generally available by OPNS to similarly entitled customers.

“Upgrade” means a major version, new generation, materially enhanced release, replacement product, new component, new commercial package, or other release that OPNS classifies as an upgrade or separately licensable release.

“Usage Data” means technical, diagnostic, operational, statistical, telemetry, performance, configuration, version, error, activation, entitlement, support, or usage-related information concerning the Products or related services.

“Use” means to install, access, run, execute, deploy, copy, configure, activate, connect, test, evaluate, operate, monitor, integrate, or otherwise use the Products or any part of them.

3. Order of Precedence

Unless expressly stated otherwise in a written agreement signed by OPNS, the following order of precedence applies in the event of conflict:

1. A specifically negotiated written agreement signed by OPNS and the relevant Customer.

2. The applicable OPNS-approved Order, quote, entitlement record, or subscription confirmation.
3. Any product-specific schedule, product terms, License Metrics, or OPNS-approved component coverage schedule expressly incorporated into the applicable Order.
4. Any support, maintenance, Corrections, Updates, End-of-Life, data processing, security, or third-party integration terms expressly incorporated into the applicable Order or this EULA.
5. Any reseller-specific terms expressly approved by OPNS and applicable to Customer's Use of the Products.
6. This EULA.
7. Documentation, only for technical or operational interpretation.

Any terms included in Customer purchase orders, procurement portals, vendor onboarding systems, administrative forms, ordering acknowledgements, emails, payment documents, or similar Customer-issued documents do not amend, supplement, waive, or override this EULA unless expressly accepted in writing by OPNS.

Where Customer obtains the Products through an Authorized Reseller, any commercial or service terms agreed between Customer and the Authorized Reseller are separate from this EULA and do not bind OPNS unless OPNS expressly accepts them in writing.

4. License Grant

Subject to Customer's compliance with this EULA, the applicable Order, the applicable Scope of Use, and payment of all applicable fees, OPNS grants Customer a limited, non-exclusive, non-transferable, non-sublicensable license to Use the Software during the applicable license term, solely for Customer's internal business purposes and solely within the applicable Scope of Use.

The Products are licensed, not sold. OPNS and its licensors retain all rights, title, and interest in and to the Products, Software, Documentation, Components, Corrections, Updates, Upgrades, configurations, technical materials, know-how, and related intellectual property rights.

No rights are granted except those expressly stated in this EULA, the applicable Order, or another written agreement signed by OPNS.

Customer does not acquire any ownership right in the Products, Software, Documentation, or any related intellectual property. All rights not expressly granted to Customer are reserved by OPNS and its licensors.

5. Scope of Use

Customer may Use the Products only:

1. For Customer's internal business purposes.
2. Within the applicable Scope of Use.
3. Within the applicable License Metrics.
4. During the applicable license term.
5. In accordance with the Documentation.
6. In the Customer Environment or another environment expressly authorized by OPNS.
7. For the Products, Components, environments, deployment models, quantities, and use cases stated in the applicable Order, entitlement record, product schedule, or OPNS-approved component coverage schedule.

Unless expressly stated otherwise in the applicable Order, Customer may not Use the Products for the benefit of any third party, as part of a managed service, outsourcing service, service bureau,

hosted offering, commercial platform, resale activity, white-label service, or other service provided to third parties.

Customer may not transfer, extend, share, pool, reuse, or apply any Product entitlement, Component, License Metric, license key, access credential, deployment right, or support entitlement outside the applicable Scope of Use.

Technical ability to install, activate, access, configure, execute, connect, copy, test, or use a Product, Component, repository, script, package, interface, Documentation, or technical material does not grant Customer any right outside the applicable Scope of Use.

6. Product Entitlement, Component Coverage, and License Metrics

Customer's Product entitlement is limited to the specific Products, Components, quantities, environments, deployment models, terms, License Metrics, and support entitlements stated in the applicable Order, quote, entitlement record, product schedule, or OPNS-approved component coverage schedule.

Each Product in the Mir.IAM product family is licensed separately. An Order, entitlement record, license key, product schedule, component coverage schedule, support entitlement, or Trial Use granted for one Product does not grant any right to Use any other Product in the Mir.IAM product family, and does not extend to shared, common, or framework Components except where OPNS makes such a Component available because it is technically required to operate the licensed Product. Access to a Mir.IAM installation package, repository, appliance image, marketplace listing, or Documentation covering more than one Product does not grant entitlement to any Product that is not expressly stated in the applicable Order.

Customer may not infer additional rights from:

1. Product names.
2. Bundle names.
3. Marketing materials.
4. Demonstrations.
5. Roadmaps.
6. Documentation.
7. Technical availability.
8. Access to installation packages.
9. Access to repositories.
10. Access to scripts, templates, libraries, or examples.
11. Prior use.
12. Authorized Reseller statements.
13. Support communications.
14. Architecture diagrams.
15. Similarity with another customer deployment.
16. Technical compatibility with another system or use case.

A Component is included only if one of the following applies:

1. It is expressly listed in the applicable Order.
2. It is expressly included in an OPNS-approved product schedule or component coverage schedule applicable to Customer.

3. OPNS expressly confirms in writing that it is included.
4. It is technically required to operate another licensed Component and OPNS makes it available for that limited purpose.

If a Component is not expressly included, it is excluded.

Customer must comply with all License Metrics stated in the applicable Order, quote, entitlement record, product schedule, or OPNS-approved component coverage schedule.

If more than one License Metric applies to a Product, Component, environment, deployment model, or use case, Customer must comply with each applicable License Metric unless OPNS expressly states otherwise in writing.

Technical ability to exceed a License Metric does not grant Customer the right to do so. Absence of technical enforcement does not waive any License Metric.

Unless expressly stated otherwise in the applicable Order, License Metrics are measured continuously during the applicable license term, and Customer must remain within the licensed scope at all times.

Where a License Metric is measured over a period, the applicable Order should specify whether the metric is measured by current active count, peak usage, average usage, monthly usage, quarterly usage, annual usage, cumulative usage, consumption during a billing period, or another agreed measurement method. If no measurement method is specified, OPNS may determine compliance based on the highest count or usage observed during the relevant period.

7. License Verification and Excess Use

Customer must maintain accurate records sufficient to demonstrate compliance with the applicable Order, Scope of Use, License Metrics, Product entitlement, and component coverage.

Upon reasonable notice, OPNS may request written confirmation, usage reports, deployment inventories, configuration extracts, system-generated reports, entitlement records, or other reasonable information to verify Customer's compliance.

Customer must cooperate reasonably with any license verification request and must not disable, bypass, manipulate, or interfere with any license key, entitlement mechanism, usage control, reporting mechanism, or technical protection measure.

If OPNS reasonably determines that Customer has exceeded the applicable Scope of Use, Product entitlement, component coverage, or License Metrics, Customer must promptly:

1. Cease the out-of-scope use.
2. Purchase the additional rights required for continued use, if OPNS agrees to make them available.
3. Pay any applicable fees for past and continuing excess use.
4. Reimburse OPNS for reasonable verification costs where material non-compliance is confirmed.

License verification must be conducted in a manner intended to minimize unreasonable disruption to Customer's operations.

Any failure by OPNS to verify usage, enforce a License Metric, or technically prevent excess use does not waive OPNS's rights or expand Customer's license.

8. Affiliates, Authorized Users, and Authorized Resellers

Customer Affiliates may Use the Products only if expressly permitted in the applicable Order, entitlement record, product schedule, or OPNS-approved component coverage schedule.

Where Affiliate use is permitted:

1. All Affiliate use counts toward the aggregate Scope of Use and applicable License Metrics.
2. Customer remains responsible for all acts and omissions of its Affiliates.
3. Customer must ensure that each Affiliate complies with this EULA.
4. No Affiliate receives any independent right to transfer, sublicense, distribute, resell, host, commercialize, or make the Products available to third parties.

Customer may permit Authorized Users to Use the Products solely on Customer's behalf and within the applicable Scope of Use.

Customer is responsible for:

1. Identifying and controlling Authorized Users.
2. Ensuring that Authorized Users comply with this EULA.
3. Maintaining the confidentiality and security of credentials, license keys, certificates, secrets, tokens, and access mechanisms.
4. All activity conducted by Authorized Users.
5. Promptly disabling access for any individual, account, credential, or service account that no longer requires access.

Authorized Resellers may access, deploy, configure, support, or otherwise handle the Products only within the scope expressly authorized by OPNS and only for the relevant Customer or End Customer. Customer remains responsible for ensuring that any Authorized Reseller acting on Customer's behalf does not exceed the applicable Scope of Use.

9. Restrictions

Customer must not, and must not permit any Affiliate, Authorized User, Authorized Reseller, service provider, or third party to:

1. Use the Products outside the applicable Scope of Use.
2. Exceed any applicable License Metric.
3. Copy the Software except as expressly permitted for backup, archival, installation, or operational purposes within the applicable Scope of Use.
4. Modify, adapt, translate, repackage, rebrand, relabel, or create derivative works of the Products.
5. Reverse engineer, decompile, disassemble, decrypt, or otherwise attempt to derive source code, underlying structure, algorithms, logic, architecture, or non-public interfaces of the Products, except to the extent such restriction is prohibited by applicable law.
6. Separate, extract, unbundle, or use any Component independently from the licensed Product or outside the licensed product scope.
7. Sublicense, sell, resell, rent, lease, lend, distribute, disclose, assign, transfer, publish, or otherwise make the Products available to any third party.
8. Host, operate, manage, or use the Products as a managed service, outsourcing service, service bureau, hosted offering, white-label service, commercial platform, platform service, or customer-facing service for third parties, unless expressly authorized in writing by OPNS.
9. Use the Products to develop, improve, train, benchmark, compare, or support a competing product or service.
10. Circumvent, disable, manipulate, or interfere with license keys, technical protection measures, usage restrictions, access controls, monitoring mechanisms, security features, reporting mechanisms, or copy-control mechanisms.

11. Remove, obscure, alter, or suppress any proprietary notices, copyright notices, trademarks, attributions, third-party notices, or license notices.
12. Publish or disclose benchmark results, performance tests, vulnerability assessments, penetration tests, security tests, comparative analyses, or similar information concerning the Products without OPNS's prior written consent.
13. Use the Products in violation of applicable laws, export controls, sanctions, data protection laws, third-party rights, or OPNS instructions.
14. Use the Products in high-risk environments where failure could lead to death, personal injury, severe property damage, environmental damage, operation of critical safety systems, weapons systems, emergency systems, or other life-critical or fail-safe environments.
15. Use the Products with unsupported versions, unsupported platforms, unsupported configurations, unsupported integrations, undocumented modifications, or unauthorized deployment models unless expressly authorized by OPNS.

Configuration of the Products within documented parameters does not transfer ownership to Customer and does not create any right to reuse, distribute, commercialize, or repurpose the Products, Components, configuration objects, scripts, templates, policies, connectors, drivers, or technical materials outside the applicable Scope of Use.

10. Customer Responsibilities

Customer is responsible for:

1. Selecting, approving, deploying, configuring, operating, monitoring, backing up, securing, and maintaining the Customer Environment.
2. Verifying that the Products meet Customer's technical, operational, legal, regulatory, security, audit, and business requirements.
3. Testing the Products, configurations, workflows, mappings, policies, synchronizations, provisioning rules, deprovisioning rules, approvals, access decisions, entitlement changes, schema extensions, Corrections, Updates, and rollback procedures before production use.
4. Maintaining accurate, complete, lawful, consistent, available, and appropriate Customer Data.
5. Obtaining and maintaining all rights, licenses, consents, approvals, credentials, certificates, APIs, accounts, permissions, third-party entitlements, and infrastructure required to use the Products.
6. Managing all identity governance decisions, access policy decisions, role model decisions, entitlement decisions, approval workflows, certification campaigns, segregation-of-duties rules, privileged access decisions, audit interpretations, and compliance decisions.
7. Reviewing, approving, testing, validating, and monitoring all configurations, mappings, workflows, policies, synchronization rules, provisioning rules, deprovisioning rules, reconciliation rules, deletion behavior, disablement behavior, rollback rules, and exception handling rules.
8. Reviewing, approving, backing up, testing, validating, and monitoring any schema extension, directory change, identity-store change, database change, or target-system change required for or affected by the Products.
9. Maintaining appropriate backups, rollback procedures, change approvals, security approvals, operational monitoring, logging, incident response procedures, and business continuity processes.
10. Ensuring that Customer's use of the Products complies with applicable law, internal policies, sector-specific requirements, audit requirements, security requirements, and contractual obligations.

11. Ensuring that its Affiliates, Authorized Users, Authorized Resellers, service providers, administrators, contractors, and other personnel comply with the applicable terms and act within the applicable Scope of Use.

Customer must not rely on default configurations, sample configurations, templates, scripts, demonstrations, reseller recommendations, support communications, documentation examples, or test results from another environment without independent validation for its own Customer Environment and use case.

OPNS is not responsible for Customer Environment, Third-Party Systems, Customer Data quality, customer or reseller configuration, insufficient testing, access policy decisions, identity governance decisions, audit interpretations, regulatory interpretations, or compliance outcomes.

11. Customer Environment, Third-Party Systems, and Integrations

The Products may connect to, depend on, read from, write to, synchronize with, provision to, reconcile with, monitor, govern, report on, or otherwise interact with Third-Party Systems and Customer Environment components.

Unless expressly agreed otherwise in writing, OPNS does not own, control, administer, monitor, secure, license, maintain, support, validate, or guarantee any Customer Environment or Third-Party System.

Customer is responsible for obtaining, maintaining, licensing, configuring, securing, monitoring, supporting, and validating all Third-Party Systems and prerequisites required for Customer's use of the Products, including systems, applications, directories, databases, APIs, IAM platforms, cloud services, operating systems, runtimes, certificates, credentials, service accounts, permissions, schemas, endpoints, data formats, network access, firewall openings, and third-party support.

OPNS is not responsible for failures, losses, malfunctions, incompatibilities, delays, outages, degraded performance, incorrect access, excessive access, missing access, incorrect provisioning, incorrect deprovisioning, incorrect deletion, incorrect disablement, failed reconciliation, workflow errors, reporting errors, governance failures, security issues, data issues, compliance issues, or support issues caused by:

1. Customer Environment.
2. Third-Party Systems.
3. Customer Data quality, accuracy, completeness, legality, format, duplication, consistency, availability, retention, or deletion.
4. Customer, Authorized Reseller, or third-party configuration.
5. Customer, Authorized Reseller, or third-party modifications.
6. Unsupported versions, unsupported platforms, unsupported integrations, unsupported deployment models, or unsupported configurations.
7. Missing prerequisites, insufficient permissions, invalid credentials, expired certificates, missing service accounts, or network restrictions.
8. API changes, schema changes, data model changes, permission changes, authentication changes, authorization changes, endpoint changes, rate limits, vendor outages, vendor defects, vendor deprecations, vendor End of Life, vendor licensing changes, or undocumented third-party behavior.
9. Customer policies, access models, role models, entitlement models, approval workflows, certification rules, reconciliation logic, synchronization rules, provisioning rules, deprovisioning rules, deletion rules, disablement rules, rollback rules, or exception handling rules.

10. Failure to test, validate, monitor, back up, secure, approve, or operate the Customer Environment or related integrations properly.
11. Unauthorized modifications, out-of-scope use, excess use, or use outside the Documentation.

Technical compatibility with a Third-Party System at one point in time does not guarantee continued compatibility.

The Products may support IAM governance, access requests, approvals, provisioning, deprovisioning, synchronization, reconciliation, role management, group management, entitlement management, certification, monitoring, reporting, and audit-related activities. OPNS does not decide who should receive access, who should lose access, which roles are appropriate, which entitlements are appropriate, which approvals are required, which exceptions should be accepted, which audit evidence is sufficient, or which compliance interpretation is correct.

Customer remains responsible for all identity governance, access policy, role model, entitlement, approval, certification, audit, security, and compliance decisions.

12. Reseller-Supplied Transactions

Customer may obtain the Products through an Authorized Reseller where OPNS permits such channel transaction.

Where Customer obtains the Products through an Authorized Reseller:

1. This EULA governs Customer's Use of the Products as between OPNS and Customer.
2. Customer's right to Use the Products remains subject to the applicable OPNS-approved Order, entitlement record, product schedule, component coverage schedule, Scope of Use, License Metrics, and Customer's compliance with this EULA.
3. Commercial terms between Customer and the Authorized Reseller are separate from this EULA.
4. The Authorized Reseller is responsible for its own pricing, invoicing, collection, statements, services, implementation, configuration, training, first-line support, customer relationship, and commercial commitments.
5. OPNS is not responsible for Authorized Reseller services, statements, warranties, commitments, support obligations, response times, service levels, implementation estimates, roadmap statements, or performance unless OPNS expressly accepts them in writing.
6. The Authorized Reseller may not grant broader rights than OPNS grants.
7. The Authorized Reseller may not modify, waive, expand, or contradict OPNS's rights or obligations unless OPNS expressly agrees in writing.
8. OPNS may provide direct support to an End Customer only where OPNS expressly agrees or where OPNS considers direct interaction appropriate for product integrity, critical troubleshooting, security, legal, operational, or country-specific reasons. Any such direct interaction does not create a general direct support obligation unless expressly agreed by OPNS.

Any unauthorized Authorized Reseller statement, commitment, warranty, assurance, representation, estimate, or promise is binding only on the Authorized Reseller and does not bind OPNS.

Authorized Resellers must not host, operate, manage, rebrand, white-label, sublicense, or provide the Products as a managed service, hosted service, outsourcing service, service bureau, platform service, or customer-facing service unless expressly authorized in writing by OPNS under a separate agreement.

Reseller-specific rights, obligations, flow-down requirements, territory, support model, hosting rights, managed service rights, payment terms, termination effects, and other reseller-specific matters are governed by the applicable agreement between OPNS and the Authorized Reseller, not by this EULA unless expressly incorporated.

13. Support Services

OPNS Support Services apply only where support has been purchased or expressly agreed in the applicable Order or another written agreement approved by OPNS.

Unless the applicable Order designates a different channel, or first-line support is provided by an Authorized Reseller, support requests concerning any Product must be submitted through the Mir.IAM support channel designated by OPNS at <https://www.mir-iam.eu/support> or by e-mail to mir.iam@opns.net, identifying the Product concerned, the Product version, the deployment model, and the environment affected. Requests submitted through other channels may be redirected to the designated channel.

Where Support Services apply, OPNS support is limited to product-level support for supported Products, supported versions, supported deployment models, supported configurations, and reproducible Product defects.

Support Services may include:

1. Technical clarification concerning supported Product behavior.
2. Analysis of reproducible Product defects.
3. Guidance on supported configurations.
4. Corrections or workarounds where OPNS determines that a supported Product does not substantially operate in accordance with the applicable Documentation.
5. Information concerning available Updates or Corrections.
6. Escalation handling according to the applicable OPNS support process.

Support Services do not include:

1. First-line support.
2. End Customer helpdesk services.
3. Implementation services.
4. Configuration services.
5. Integration services.
6. Project management.
7. Training.
8. Custom development.
9. Customer-specific workflow design.
10. Role model design.
11. Access policy design.
12. Entitlement design.
13. Compliance advice.
14. Audit interpretation.
15. Customer Environment administration.
16. Third-Party System administration.
17. Data cleansing.
18. Backup, restore, disaster recovery, or business continuity services.

19. Monitoring of Customer systems.
20. Security monitoring of Customer systems.
21. Resolution of customer-caused, reseller-caused, or third-party-caused issues.
22. Support for unsupported versions, unsupported platforms, unsupported integrations, unsupported configurations, or unsupported modifications.
23. Support for out-of-scope use or excess use.

OPNS may suspend, refuse, redirect, limit, or condition Support Services where:

1. Support entitlement is inactive.
2. Applicable fees are unpaid.
3. The Product is used outside the applicable Scope of Use.
4. Customer exceeds applicable License Metrics.
5. The issue relates to unsupported versions, unsupported configurations, unsupported integrations, unsupported modifications, Customer Environment, Third-Party Systems, Customer Data quality, Authorized Reseller services, or out-of-scope use.
6. Required information is not provided.
7. Customer or Authorized Reseller fails to cooperate reasonably.
8. Continued support would create security, legal, operational, or compliance risk for OPNS.

Customer and, where applicable, Authorized Reseller must cooperate reasonably with OPNS support activities, including by providing accurate information, logs, diagnostic materials, reproduction steps, configuration details, version details, entitlement details, and access to qualified personnel where reasonably required.

OPNS does not guarantee that every issue will be corrected, that every workaround will be suitable for Customer's environment, or that Support Services will resolve issues caused by factors outside OPNS control.

14. Corrections, Updates, Upgrades, and Supported Versions

Customer is entitled to Corrections and Updates only where Customer has an active support or maintenance entitlement covering the affected Product.

OPNS may determine, in its reasonable discretion, whether an issue requires a Correction, workaround, configuration guidance, documentation clarification, Update recommendation, security-related Update, escalation, or no action.

Corrections may include bug fixes, patches, workarounds, minor updates, configuration guidance, documentation clarification, or other changes made available by OPNS to address reproducible defects in the Software.

Updates may include Corrections, maintenance releases, minor versions, compatibility updates, security-related updates, documentation updates, or technical improvements made generally available by OPNS to similarly entitled customers.

Unless expressly stated otherwise in the applicable Order, Updates do not include Upgrades, new Products, new commercial packages, separately licensed Components, separately priced modules, Professional Services, customer-specific development, or migration services.

Customer is not entitled to receive Upgrades unless expressly agreed in the applicable Order or another written agreement approved by OPNS.

OPNS may classify a release, major version, new generation, materially enhanced release, replacement product, new Component, new commercial package, or other release as an Upgrade.

An Upgrade may be subject to additional fees, additional terms, additional License Metrics, technical prerequisites, migration requirements, or a separate Order.

Support, Corrections, Updates, security-related Updates, compatibility maintenance, and technical analysis may be limited to Supported Versions. OPNS may refuse, limit, suspend, or condition support, Corrections, or Updates for unsupported versions, End-of-Life versions, unsupported deployment models, unsupported configurations, unauthorized modifications, or versions for which required Corrections or Updates have not been installed.

Unless expressly agreed otherwise in writing, Customer is responsible for installing, applying, testing, validating, operating, backing up, monitoring, and maintaining all Corrections and Updates in the Customer Environment.

Customer must assess the impact of any Correction or Update before production deployment and remains responsible for backups, rollback readiness, change approvals, security approvals, non-production testing, compatibility with Customer Environment, compatibility with Third-Party Systems, validation of workflows, validation of mappings, validation of provisioning logic, validation of deprovisioning logic, validation of governance processes, production deployment timing, and post-installation monitoring.

OPNS is not responsible for loss, disruption, misconfiguration, access errors, data issues, workflow errors, provisioning errors, deprovisioning errors, security issues, or compliance issues caused by Customer's or Authorized Reseller's failure to test, validate, approve, install, operate, secure, or monitor Corrections or Updates properly.

Security-related Updates, mitigations, workarounds, technical guidance, or configuration recommendations do not create a general security monitoring obligation, managed security service, incident response obligation, or guarantee that OPNS will detect, prevent, remediate, or be responsible for security incidents in the Customer Environment or Third-Party Systems.

15. End of Life

OPNS may modify, replace, supersede, discontinue, restrict availability, or end support for any Product, Component, version, feature, platform, integration, deployment model, technical dependency, or Documentation set.

Where commercially reasonable, OPNS may provide notice before a Product, Component, version, feature, platform, integration, or deployment model reaches End of Life. Unless expressly stated otherwise in the applicable Order, failure to provide a specific notice period does not prevent OPNS from discontinuing development, support, Corrections, Updates, compatibility maintenance, or availability where OPNS considers discontinuation necessary for product, security, legal, technical, operational, third-party dependency, or commercial reasons.

After End of Life, OPNS may stop providing, for the affected item:

1. Support.
2. Corrections.
3. Updates.
4. Security-related Updates.
5. Compatibility updates.
6. Maintenance releases.
7. Documentation updates.
8. Technical troubleshooting.
9. Escalation handling.
10. Platform certification.

11. Integration maintenance.
12. Replacement packages.
13. Download availability.
14. New license sales.
15. Subscription sales.
16. Renewal availability.

OPNS may require Customer or Authorized Reseller to migrate to a Supported Version, replacement Product, replacement Component, supported platform, supported integration, or supported deployment model before OPNS provides further support or analysis.

Unless expressly agreed in writing by OPNS, OPNS has no obligation to maintain, update, correct, secure, test, certify, distribute, or support any End-of-Life Product, Component, version, feature, platform, integration, deployment model, or technical dependency.

Customer is responsible for planning, testing, validating, approving, funding, implementing, securing, and operating any migration required as a result of End of Life. Migration assistance is not included unless expressly agreed in a statement of work, Order, or other written agreement approved by OPNS.

End of Life does not entitle Customer to receive an Upgrade, replacement Product, migration service, custom development, refund, credit, or extension unless expressly agreed in writing by OPNS.

Unless the applicable license term has expired or OPNS terminates the relevant rights, End of Life does not automatically terminate Customer's license to use a perpetual license for the affected Software within the applicable Scope of Use.

However, continued use after End of Life is at Customer's own risk and without OPNS support, Corrections, Updates, security-related Updates, compatibility maintenance, or warranty, unless OPNS expressly agrees otherwise in writing.

16. Customer Data, Usage Data, and Data Protection

Customer retains ownership of Customer Data.

OPNS's processing of personal data in connection with the Mir.IAM websites, Product trial and license key requests, support requests, and lead information received from online marketplaces is described in the Mir.IAM Privacy Policy available at <https://www.mir-iam.eu/privacy>. The Privacy Policy is informational, describes OPNS's processing as controller of its own business contact and website data, and does not amend, expand, or limit these Software License Terms or any data processing terms expressly incorporated into the applicable Order.

Customer grants OPNS the limited right to use Customer Data only as necessary to provide the Products, Support Services, Professional Services, Corrections, Updates, troubleshooting, security analysis, license verification, or other services expressly agreed with Customer.

Customer remains responsible for the accuracy, completeness, legality, quality, relevance, retention, deletion, security, and lawful processing of Customer Data.

This section applies to Personal Data only where OPNS processes Personal Data on behalf of Customer or End Customer in connection with the Products, Support Services, Professional Services, or other OPNS services expressly covered by the applicable Order.

This section does not apply to:

1. Personal Data processed solely in the Customer Environment.

2. Personal Data processed solely in Third-Party Systems.
3. Personal Data processed solely in reseller systems.
4. Personal Data processed by an Authorized Reseller as an independent service provider.
5. Customer Data that OPNS does not access, receive, host, store, transmit, or otherwise process.
6. Usage Data that has been aggregated or de-identified so that it no longer identifies Customer, End Customer, or individuals.
7. OPNS processing of business contact information for its own account management, billing, legal, security, or commercial administration purposes.

Customer is responsible for determining the purposes of processing, categories of Personal Data, data subjects concerned, lawful basis, retention periods, access rights, identity governance rules, and whether the Products and related processing meet Customer's legal, regulatory, security, and operational requirements.

Where OPNS processes Personal Data on behalf of Customer, OPNS will process it only in accordance with the applicable Order, Customer's documented instructions, this EULA, and applicable law.

Customer must not provide OPNS with Regulated Data unless:

1. The applicable Order expressly permits it.
2. The processing is necessary for the agreed services.
3. Appropriate safeguards have been agreed in writing.
4. Customer has confirmed that the processing is lawful.
5. Any required additional terms have been executed.

OPNS may reject, delete, return, restrict, or require redaction of Regulated Data that is provided without the required authorization.

Support Data may include logs, configuration extracts, screenshots, diagnostic files, error messages, traces, system information, identity records, account information, workflow extracts, or other materials provided to OPNS for support or troubleshooting. Customer must avoid providing Personal Data, confidential data, secrets, credentials, access tokens, private keys, Regulated Data, or production data in Support Data unless necessary for the support request and lawfully permitted.

OPNS may collect and use Usage Data for support, security, license administration, product maintenance, product improvement, analytics, operational reporting, troubleshooting, and abuse prevention.

OPNS may use aggregated or de-identified Usage Data for any lawful business purpose, provided it does not identify Customer, End Customer, or individuals.

Where legally required and taking into account the nature of the processing and the information available to OPNS, OPNS will provide reasonable assistance to Customer for data subject requests, security of processing, Data Breach assessment, data protection impact assessments, and prior consultation with supervisory authorities. OPNS's assistance is limited to Personal Data processed by OPNS on behalf of Customer.

OPNS is not responsible for Customer's compliance program, audit conclusions, legal interpretations, regulator communications, risk assessments, governance model, access controls, Customer Environment security, identity governance decisions, access policy decisions, data retention decisions, legal basis decisions, data quality, data minimization, or compliance outcomes.

OPNS will not sell Personal Data processed on behalf of Customer. OPNS will not use Personal Data processed on behalf of Customer for advertising, profiling for third-party commercial purposes, or unrelated commercial exploitation. This does not restrict OPNS from using aggregated or de-identified Usage Data as permitted in this EULA.

17. Security Responsibilities

OPNS will apply appropriate technical and organizational measures designed to protect the Products and OPNS-controlled environments against unauthorized access, alteration, disclosure, or destruction.

OPNS security obligations are limited to Products supplied by OPNS, OPNS-controlled environments, Support Services provided by OPNS, Personal Data actually processed by OPNS, Customer Data actually received by OPNS, and security commitments expressly accepted by OPNS in writing.

Customer is responsible for securing the Customer Environment, including infrastructure, servers, endpoints, networks, directories, databases, applications, cloud tenants, containers, virtual machines, operating systems, credentials, secrets, certificates, tokens, service accounts, API accounts, administrator accounts, access controls, roles, groups, workflows, approval rules, governance processes, backups, monitoring, logging, and incident response.

OPNS is not responsible for security issues caused by:

1. Customer Environment.
2. Third-Party Systems.
3. Authorized Reseller services.
4. Customer or Authorized Reseller configuration.
5. Unsupported modifications.
6. Unsupported versions.
7. Unsupported deployment models.
8. Use outside the Documentation.
9. Use outside the applicable Scope of Use.
10. Failure to install Corrections or Updates.
11. Failure to apply security-related Updates or mitigations.
12. Insufficient access controls.
13. Weak credentials.
14. Expired certificates.
15. Incorrect permissions.
16. Network exposure.
17. Insecure infrastructure.
18. Customer Data quality issues.
19. Customer identity governance decisions.
20. Customer access policy decisions.

The Products, Support Services, Corrections, Updates, security-related Updates, technical guidance, or support communications do not constitute managed security services, security monitoring services, incident response services, security operations center services, compliance monitoring services, audit services, legal advice, regulatory advice, cybersecurity certification, or identity governance certification.

OPNS may provide security-related Updates, Corrections, workarounds, mitigations, configuration guidance, or technical recommendations. Customer and Authorized Reseller must reasonably cooperate with OPNS where OPNS identifies or reasonably suspects a security issue affecting the Products.

OPNS may require Customer or Authorized Reseller to install a security-related Update, apply a Correction, apply a workaround, disable an unsafe configuration, move to a Supported Version, remove unsupported modifications, restrict access, provide logs or diagnostic information, or complete reasonable security validation steps.

18. Security Incidents, Vulnerability Reports, and Security Testing

Where OPNS confirms a Security Incident affecting OPNS-controlled environments, Products under OPNS control, or Personal Data processed by OPNS on behalf of Customer, OPNS will notify Customer without undue delay.

The notice will include information reasonably available to OPNS, taking into account the nature of the Security Incident, applicable legal requirements, and any need to protect security, confidentiality, investigation integrity, or third parties.

OPNS's notification of a Security Incident is not an admission of fault, liability, breach of contract, or breach of law.

Customer remains responsible for determining whether notification to regulators, data subjects, employees, customers, auditors, insurers, or other third parties is required.

This section does not apply to incidents occurring solely in the Customer Environment, Third-Party Systems, Authorized Reseller systems, End Customer systems not controlled by OPNS, or other environments not controlled by OPNS.

Customer, Authorized Reseller, or a third party may report suspected vulnerabilities to OPNS through the channel designated by OPNS. A vulnerability report must include sufficient technical information for OPNS to assess the issue, including affected Product, affected version, deployment model, configuration details relevant to the issue, reproduction steps, logs or technical evidence where available, potential impact, known exploitation where applicable, and contact details for follow-up.

The channel designated by OPNS for vulnerability reports is the Mir.IAM support channel at <https://www.mir-iam.eu/support> or mir.iam@opns.net, marked for the attention of product security. OPNS will acknowledge a report that contains the information described above and will inform the reporter of the outcome of its assessment.

OPNS may determine whether the reported issue is a Product vulnerability, a configuration issue, a Customer Environment issue, a Third-Party System issue, an unsupported use issue, or not reproducible.

Customer and Authorized Reseller must not publicly disclose suspected vulnerabilities, exploit details, security test results, vulnerability reports, or similar information concerning the Products without OPNS's prior written consent, unless disclosure is required by applicable law.

Customer must not perform penetration testing, vulnerability scanning, exploit testing, load testing, security testing, or similar testing against OPNS-controlled environments without OPNS's prior written approval.

Security testing in the Customer Environment remains Customer's responsibility, but must not violate this EULA, attempt to reverse engineer the Products, circumvent license controls, access OPNS systems without authorization, interfere with OPNS systems or other customers, publicly

disclose results without OPNS's prior written consent, or use the Products for unlawful or harmful activity.

19. No Expansion of Obligations

Support communications, troubleshooting, Corrections, workarounds, Updates, security-related Updates, configuration suggestions, technical guidance, lifecycle communications, migration recommendations, replacement recommendations, data protection assistance, security assistance, incident communications, or vulnerability handling do not expand Customer's license rights, Product entitlement, component coverage, License Metrics, support entitlement, security entitlement, data protection rights, authorized deployment scope, or OPNS obligations.

Any expansion of rights, services, support obligations, security obligations, data processing obligations, hosting obligations, managed service obligations, direct End Customer support obligations, migration services, custom development, or compliance commitments must be expressly approved by OPNS in the applicable Order or another written agreement signed by OPNS.

20. Intellectual Property, Feedback, and Product Materials

OPNS and its licensors retain all rights, title, and interest in and to the Products, Software, Documentation, Components, Corrections, Updates, Upgrades, configurations, technical materials, know-how, trade secrets, and related intellectual property rights.

Customer does not acquire ownership of the Products, Software, Documentation, Components, or any related intellectual property rights.

Customer receives only the limited license rights expressly granted under this EULA, the applicable Order, or another written agreement signed by OPNS.

Customer must not remove, obscure, alter, suppress, or interfere with any copyright notice, trademark, proprietary notice, attribution, third-party notice, license notice, digital signature, license key, entitlement marker, or technical protection measure included in or with the Products.

If Customer, an Affiliate, an Authorized User, an Authorized Reseller, or an End Customer provides feedback, suggestions, ideas, enhancement requests, recommendations, corrections, or other comments concerning the Products, OPNS may use them without restriction, obligation, attribution, or compensation.

No feedback, support request, enhancement request, configuration suggestion, bug report, roadmap discussion, or technical exchange transfers ownership of the Products, creates joint ownership, or grants Customer any right to OPNS improvements, Corrections, Updates, Upgrades, know-how, methods, or reusable components.

21. Confidentiality

Each party must protect the other party's Confidential Information using at least reasonable care and must use such Confidential Information only for purposes related to the contractual relationship.

"Confidential Information" means non-public information disclosed by or on behalf of a party that is identified as confidential or should reasonably be understood to be confidential given the nature of the information or the circumstances of disclosure.

The Products, Software, Documentation, license keys, object code, source code, architecture, logic, configurations, non-public APIs, technical materials, security information, vulnerability information, product roadmaps, pricing, entitlement information, support communications, and non-public product information are OPNS Confidential Information.

Confidentiality obligations do not apply to information that the receiving party can demonstrate:

1. Is publicly available without breach of this EULA.
2. Was lawfully known before receipt.
3. Was independently developed without use of the disclosing party's Confidential Information.
4. Was lawfully received from a third party without confidentiality obligation.
5. Must be disclosed under applicable law, court order, or regulatory requirement, provided that the receiving party gives reasonable prior notice where legally permitted.

Customer must ensure that its Affiliates, Authorized Users, Authorized Resellers, service providers, and personnel protect OPNS Confidential Information in accordance with this EULA.

Nothing in this section limits Customer's license restrictions, security obligations, data protection obligations, or obligation to protect the Products and related OPNS materials.

22. Third-Party Materials

The Products may include, be distributed with, require, or interoperate with Third-Party Materials.

Third-Party Materials may be subject to separate license terms, notices, restrictions, support terms, or usage conditions. To the extent required by applicable third-party terms, those terms govern Customer's use of the relevant Third-Party Materials.

Nothing in this EULA limits rights that Customer may have under open-source licenses that cannot lawfully be restricted.

OPNS does not grant broader rights to Third-Party Materials than OPNS is legally permitted to grant.

Except where expressly required by applicable law or by the relevant third-party license, OPNS disclaims responsibility for Third-Party Materials and Third-Party Systems.

Customer is responsible for complying with third-party terms, maintaining required third-party licenses, and ensuring that Customer's use of Third-Party Materials and Third-Party Systems is lawful and compatible with the applicable Scope of Use.

23. Warranty Disclaimer

To the maximum extent permitted by applicable law, the Products, Software, Documentation, Components, Corrections, Updates, Upgrades, Support Services, Professional Services, Third-Party Materials, technical guidance, and any related materials are provided "as is" and "as available", unless an express written warranty is stated in the applicable Order or another written agreement signed by OPNS.

OPNS disclaims all implied, statutory, or other warranties, conditions, representations, and commitments, including warranties of merchantability, fitness for a particular purpose, non-infringement, uninterrupted operation, error-free operation, security, compatibility, availability, accuracy, completeness, compliance, and suitability for Customer's intended use.

OPNS does not warrant that the Products will:

1. Meet Customer's requirements.
2. Operate without interruption or error.
3. Operate with all Third-Party Systems.
4. Remain compatible with future third-party changes.
5. Prevent unauthorized access or security incidents.
6. Produce correct access decisions, governance decisions, audit conclusions, or compliance results.

7. Achieve any legal, regulatory, security, operational, governance, audit, or business outcome.

Any limited warranty expressly accepted by OPNS does not apply to issues caused by Customer Environment, Third-Party Systems, Customer Data, Customer or Authorized Reseller configuration, unauthorized modification, unsupported versions, unsupported platforms, unsupported integrations, unsupported deployment models, misuse, negligence, accident, out-of-scope use, failure to follow Documentation, insufficient testing, or evaluation, trial, beta, preview, demonstration, or pre-release use.

24. Limitation of Liability

To the maximum extent permitted by applicable law, OPNS will not be liable for indirect, incidental, special, consequential, exemplary, punitive, or similar damages, including loss of profits, revenue, business, goodwill, anticipated savings, data, use, access, security, reputation, or business interruption, even if OPNS has been advised of the possibility of such damages.

To the maximum extent permitted by applicable law, OPNS will not be liable for damages, losses, costs, claims, penalties, or expenses arising from:

1. Customer Environment.
2. Third-Party Systems.
3. Customer Data quality, legality, accuracy, completeness, retention, deletion, or availability.
4. Customer or Authorized Reseller configuration.
5. Customer or Authorized Reseller services, statements, warranties, commitments, or support.
6. Insufficient testing, missing backups, missing rollback procedures, or unsupported deployment.
7. Access policy decisions, role model decisions, entitlement decisions, approval decisions, governance decisions, audit interpretations, or compliance outcomes.
8. Security incidents not caused by a proven breach by OPNS of an obligation expressly accepted by OPNS.
9. Regulatory penalties or sanctions arising from Customer's use, configuration, data, environment, or decisions.
10. Use outside the applicable Scope of Use.

To the maximum extent permitted by applicable law, OPNS's aggregate liability arising out of or relating to the Products, Software, Support Services, Professional Services, Orders, or this EULA will not exceed the amounts paid to OPNS for the affected Product or service during the twelve (12) months preceding the event giving rise to liability.

For evaluation, trial, beta, preview, demonstration, free, or pre-release use, OPNS's aggregate liability is limited to fifty euros (EUR 50), to the maximum extent permitted by applicable law.

Nothing in this EULA excludes or limits liability to the extent such exclusion or limitation is prohibited by mandatory applicable law.

25. Term, Suspension, and Termination

The license term is stated in the applicable Order.

If the license is subscription-based, term-based, evaluation, trial, beta, preview, demonstration, or otherwise time-limited, Customer's right to Use the Products ends when the applicable term expires, unless renewed or extended by OPNS in writing.

OPNS may suspend Customer's access to the Products, license keys, support, Updates, Corrections, or related services where Customer:

1. Fails to pay applicable fees.
2. Exceeds the applicable Scope of Use or License Metrics.
3. Uses the Products unlawfully or in breach of this EULA.
4. Violates license restrictions.
5. Creates security, legal, operational, product integrity, or compliance risk.
6. Fails to cooperate with reasonable support, security, license verification, or remediation requests.
7. Uses unsupported, unauthorized, or unsafe configurations in a manner that may affect OPNS, the Products, or third parties.

OPNS may terminate Customer's license or the affected Order if Customer materially breaches this EULA and fails to cure the breach within thirty (30) days after notice, unless the breach is incapable of cure or requires faster action to protect OPNS, the Products, security, intellectual property, or legal compliance.

OPNS may terminate immediately where Customer infringes OPNS intellectual property rights, misuses Confidential Information, circumvents license controls, reverse engineers the Products, sublicenses or distributes the Products without authorization, uses the Products for unlawful purposes, or materially exceeds the applicable Scope of Use.

Upon expiration or termination of the applicable license, Customer must:

1. Stop using the affected Products.
2. Delete or return all copies under its control.
3. Stop using related Components, Documentation, license keys, credentials, and OPNS materials.
4. Stop all production, non-production, disaster recovery, hosted, managed service, or other use of the affected Products.
5. Certify compliance upon OPNS request.
6. Pay all amounts due for use before termination or expiry.

Termination does not entitle Customer to any refund, credit, or reimbursement unless expressly required by mandatory applicable law or agreed in writing by OPNS.

26. Export Control, Sanctions, and Legal Compliance

Customer must comply with all applicable export control, sanctions, embargo, trade compliance, import, deployment, privacy, security, labor, public sector, and sector-specific laws and regulations.

Customer must not export, re-export, transfer, provide access to, or use the Products in violation of applicable export control or sanctions laws, or for prohibited end users, end uses, or territories.

Customer must not use the Products in connection with unlawful activity, sanctioned activity, restricted persons, restricted entities, restricted jurisdictions, or prohibited end uses.

Customer is responsible for obtaining all required licenses, approvals, authorizations, consents, registrations, and permits relating to export, re-export, transfer, access, deployment, or use of the Products.

OPNS may suspend or terminate access, support, delivery, Updates, Corrections, or other performance where OPNS reasonably determines that continued performance may violate applicable law, sanctions, export controls, or regulatory requirements.

27. Assignment and Subcontracting

Customer may not assign, transfer, delegate, or novate this EULA, any Order, or any rights to the Products without OPNS's prior written consent.

Any attempted assignment or transfer in violation of this section is void.

OPNS may assign, transfer, delegate, or novate its rights and obligations to an Affiliate, successor, acquirer, or entity involved in a merger, reorganization, transfer of assets, transfer of business activities, or similar transaction.

OPNS may use subcontractors, service providers, hosting providers, support providers, security providers, communication providers, ticketing providers, professional advisers, and other third parties to perform obligations or exercise rights under this EULA, provided that OPNS remains responsible for obligations expressly accepted by OPNS and subject to applicable confidentiality and data protection requirements.

28. Governing Law, Jurisdiction, and Language

This EULA and any dispute arising out of or relating to it are governed by the laws of Belgium, excluding conflict-of-law rules.

The courts competent for OPNS's registered office have exclusive jurisdiction over disputes arising out of or relating to this EULA, unless mandatory applicable law requires otherwise.

The English version of this EULA controls, unless mandatory applicable law requires otherwise or OPNS expressly agrees to another language precedence in writing.

The United Nations Convention on Contracts for the International Sale of Goods does not apply.

Nothing in this EULA limits rights, remedies, or obligations that cannot be excluded or limited under mandatory applicable law.

29. General Legal Terms

This EULA, the applicable Order, and any written terms expressly incorporated by OPNS constitute the agreement governing Customer's Use of the Products.

Customer purchase orders, procurement terms, vendor portal terms, administrative documents, click-through terms, emails, acknowledgements, payment documents, or other Customer-issued terms do not modify the agreement unless expressly accepted in writing by OPNS.

Customer acknowledges that its purchase is not contingent on delivery of future functionality, roadmap items, product plans, public statements, demonstrations, or statements not expressly included in the applicable Order.

If any provision of this EULA is held invalid or unenforceable, the remaining provisions remain in effect, and the invalid or unenforceable provision will be interpreted or replaced to achieve the closest lawful effect.

Failure to enforce a provision does not waive the right to enforce it later.

Neither party is responsible for delay or failure to perform caused by events beyond its reasonable control, except that this does not excuse payment obligations, license restrictions, confidentiality obligations, data protection obligations, security obligations, or obligations relating to unauthorized use of the Products.

Legal notices to OPNS must be sent to the address specified in the applicable Order or in OPNS's official notice details made available to Customer. Operational support requests, product questions, reseller communications, and ordinary business communications are not legal notices unless expressly identified as legal notices and sent through the required notice channel.

Sections concerning license restrictions, ownership, confidentiality, payment obligations, license verification, disclaimers, limitation of liability, Customer responsibilities, Third-Party Systems, data protection, security, termination effects, export control, governing law, and any provisions that by their nature should survive will survive expiration or termination.

No person or entity other than OPNS, Customer, and their permitted successors and assigns has rights under this EULA, except that OPNS affiliates and licensors may enforce provisions protecting the Products, intellectual property, Confidential Information, license restrictions, disclaimers, and limitations of liability.

Execution (Optional — Negotiated Signature)

Acceptance of these Software License Terms occurs as set out in Section 1 (by installing, accessing, deploying, or using the Products, or through an Order that incorporates this EULA). Signature below is required only where OPNS and Customer elect to enter into a signed agreement. Where signed, this page forms part of, and is governed by, these Software License Terms and the applicable Order.

For and on behalf of OPNS SA/NV	For and on behalf of the Customer
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____
Signature: _____	Signature: _____

Annex A — Mir.IAM Product Family

This Annex identifies the Products forming part of the Mir.IAM product family as at the Effective Date of these Software License Terms. It is descriptive only. Customer's Product entitlement, Components, License Metrics, quantities, environments, deployment models, term, and support entitlement are determined solely by the applicable Order, quote, entitlement record, product schedule, or OPNS-approved component coverage schedule, as set out in Sections 1, 5, and 6.

- **LARA — Lightweight Access Review Application.** Web-based access review and certification campaigns. Reads users and their entitlements directly from an LDAP data source into a campaign snapshot, presents one review page per reviewer, records approve, revoke, and escalate decisions per entitlement, and produces a signed closure report, machine-readable exports, and optional LDAP fulfilment.
- **MAYA — Manage All Your Applications.** Application onboarding into the identity governance model, covering the declaration of applications and their access rights and the associated provisioning and governance Components.
- **PAUL — Protect & Audit Ubiquitous Libraries.** Protection and audit of critical identity management activity, including detection of abnormal transaction volumes and the centralisation of operational evidence.

- **SARA — Smart Access Rights Automation.** Automation of standard joiner, mover, and leaver access-right assignment, cleanup, and review readiness, including grace-period handling.
- **ZETI — Zero Trust Improvements.** Least-privilege enforcement in identity management environments, including privilege drift detection and local administrator governance.

OPNS may add a Product to, remove a Product from, rename a Product within, or reorganise the Mir.IAM product family, and may make a Product available as part of a bundle or as a separately licensable Product. Any such change applies to Orders placed after the change and does not alter Customer's existing Product entitlement for the remainder of the applicable license term. The current composition of the Mir.IAM product family is published at <https://www.mir-iam.eu/products>.

Each Product listed in this Annex is licensed separately. Nothing in this Annex grants Customer any right to Use a Product that is not expressly stated in the applicable Order.

Annex B — Trial Use, Evaluation, and Marketplace Distribution

This Annex applies to all Trial Use of any Product, including Trial Use obtained through an online marketplace listing operated by a third party such as the Microsoft commercial marketplace, through a trial license key issued by OPNS, or through a download made available on an OPNS or Mir.IAM website. Where this Annex conflicts with another provision of these Software License Terms, this Annex prevails for the duration of the Trial Use and to the extent of the conflict.

Grant and scope of Trial Use

- OPNS grants Customer a limited, non-exclusive, non-transferable, non-sublicensable, revocable license to Use the Product identified in the trial confirmation, solely for the purpose of internally evaluating that Product, and solely within the trial term.
- Trial Use is permitted in a non-production environment only. Trial Use in a production environment, for production identity governance decisions, or for the benefit of any third party is not permitted.
- Unless OPNS states a different period in writing, the trial term is thirty (30) days from the date the trial license key is issued. OPNS may extend, shorten, suspend, or terminate a trial term at any time at its discretion.
- Trial Use covers only the Product for which the trial license key was issued. A trial of one Product does not grant any right to Use any other Product in the Mir.IAM product family.
- One trial per Customer legal entity per Product applies unless OPNS agrees otherwise in writing. Requesting repeat or overlapping trials to extend evaluation beyond the trial term is not permitted.

Customer obligations during Trial Use

- Customer remains responsible for the Customer Environment, Third-Party Systems, Customer Data, configuration, testing, backups, rollback readiness, and security during Trial Use, as set out in Sections 10, 11, and 17.
- Customer must not enable LDAP fulfilment, automated revocation, provisioning, deprovisioning, or any other write-back function against a production directory during Trial Use without first testing it in a non-production environment and taking its own backups.
- Customer must provide accurate registration information when requesting a trial, including a business e-mail address and the legal entity on whose behalf the trial is requested.
- At the end of the trial term Customer must cease all Use of the Product, delete or return all copies under its control, and stop using the associated license keys, credentials, and OPNS materials, unless Customer has by then obtained a paid license under an applicable Order.

No warranty, no support commitment, limited liability

- Products under Trial Use are provided “as is” and “as available”, without warranty of any kind, as set out in Section 23. No express or implied warranty applies to Trial Use.
- Support Services are not included with Trial Use. OPNS may, at its discretion, provide installation guidance or answer questions during a trial, and any such assistance does not create a support entitlement, a service level, or any obligation under Section 13.
- For all Trial Use, OPNS's aggregate liability is limited to fifty euros (EUR 50), to the maximum extent permitted by applicable law, as set out in Section 24.
- OPNS gives no commitment that a Product evaluated under Trial Use will remain available, will retain any particular feature, or will be offered on any particular commercial terms.

Marketplace listings and lead information

- Where Customer reaches a Product through an online marketplace listing, the marketplace operator is an independent third party. The marketplace operator's terms govern Customer's use of the marketplace itself; these Software License Terms govern Customer's Use of the Product.
- A marketplace listing, listing description, category, screenshot, plan name, price indication, or trial button does not grant any right beyond the rights expressly granted in these Software License Terms and the applicable Order, and does not create any warranty, support commitment, service level, or entitlement, as set out in Sections 1 and 6.
- Where Customer requests information or a trial through a marketplace listing, the marketplace operator may transmit Customer's registration and contact details to OPNS so that OPNS can respond. OPNS processes those details as described in the Mir.IAM Privacy Policy at <https://www.mir-iam.eu/privacy>.
- OPNS is not responsible for the availability, content, accuracy, categorisation, ranking, billing, or operation of any third-party marketplace, or for any statement, commitment, or term presented by a marketplace operator that OPNS has not expressly accepted in writing.

Conversion to a paid license

Trial Use does not convert automatically into a paid license and does not create any obligation on either party to enter into an Order. Where Customer subsequently obtains a paid license for the Product, these Software License Terms continue to apply, this Annex ceases to apply from the start date stated in the applicable Order, and the Scope of Use, License Metrics, term, and support entitlement stated in that Order govern from that date.