Denodo Vendor Assessment - Interpretation Guidelines

INTRODUCTION

Denodo is an independent software provider which develops and markets a COTS (commercial off-the-shelf) solution, the Denodo Platform (including related add-ons, herein referred to as the "Denodo Platform").

The Denodo Platform, powered by Data Virtualization, is the leading Data Integration, Management and Delivery Platform using a Logical Approach. The Denodo Platform connects to data sources – be they structured, semi-structured or unstructured, internal or external – and combines them into logical / virtual data services to provide unified access and integrated delivery through a single "virtual" data layer. The virtual data layer can be published to consuming applications in real-time (right-time). It includes key capabilities for real-time query optimization supported by intelligent caching and scheduled data orchestration, unified data governance and quality, and ability to deliver data services in multiple formats with managed security and service-levels.

As a COTS solution, the Denodo Platform is not tailored to a specific customer, but it is provided as is to all our customers. Denodo must at all times remain able to provide its software to different companies, even if they are in competition with each other.

Data virtualization is the modern approach to data integration. Unlike ETL solutions, which replicate data, data virtualization leaves the data in source systems, simply exposing an integrated view of all the data to data consumers.

Data Virtualization main characteristics are:
1. **Data abstraction:** Data virtualization hides the complexities of accessing data from the underlying data systems, their formats and structures.
2. **Zero replication:** Unlike ETL, data virtualization does not need to "collect" the data into a separate repository in order to transform it to the destination format. It handles the transformation and aggregation on-the-fly.
3. **Real-time data delivery:** Since data virtualization "connects" to the underlying data sources in real-time, it delivers up-to-the-minute data to the business users within their applications.
4. **Agility and simplicity:** Data virtualization's view-based approach delivers agility when underlying sources are added, removed, or changed.

Find more information about this at https://www.denodo.com/en/data-virtualization/benefits

SCOPE OF DENODO PRODUCTS & SERVICES

The Product & Services Denodo provides to our customers are the following:
1. **Licenses** for the Denodo Platform software.
2. **Support and maintenance services** for the Denodo Platform software.
3. **Training and Consultancy services** to help our customers and/or their preferred partners to implement data virtualization solutions, based on the Denodo Platform software, and adapted to satisfy the needs of the organization.

The following services are out of the scope of Denodo's offering:
1. **Hosted/cloud environment** where the Denodo Platform runs in Denodo owned facilities or 3-party facilities managed by Denodo. The Denodo Platform **is not SaaS**.
2. **Full Implementation services** of Data Virtualization solutions based on the Denodo Platform at the customer. Note: Denodo's services can assist our customers during the implementation.
3. **Operation and maintenance** of Data Virtualization solutions based on the Denodo Platform at the customer.

REMARKS

Denodo Vendor Assessment - Interpretation Guidelines

The Denodo Platform is a software solution that **will be installed on-premise at the customer's facilities or where the customer decides, including public/private cloud services such as AWS, Azure or GCP**.

Denodo does not provide, operate, or maintain the environment where the Denodo Platform runs. Denodo does not yet market a SaaS solution. Denodo does not subcontract 3-party suppliers for this purpose either. It is the customer's responsibility to assess the environment to meet company SLAs and regulatory security and privacy standards.

In addition, **no Denodo system nor personnel (at Denodo facilities or 3-party facilities managed by Denodo), nor other companies/persons on behalf of Denodo, do access/process/store customer's data, nor do any connection be established with the customer's computer networks and systems. Denodo is not a data "Processor" nor provide data "Processor" services to the customers.**

VENDOR ASSESSMENT INTERPRETATION GUIDELINES

Taking into account the scoped product and services, we distinguish three different levels from a Information Security perspective:

1. **High Risk** - In the first level, and more important for our customers, we place the security of the **Denodo Platform Software Development Life Cycle (SDLC)** process. Though Denodo is not responsible for the solution deployed at our customers, hence it corresponds to the customer to protect the environment against vulnerabilities, the Denodo Platform aims to be the central and unique point within the organization to access data for business. As such, the Denodo Platform can have access to data sources across and beyond the walls of the organization, and all its data is susceptible to pass through the Denodo Platform. Knowing that, Denodo has put in place strict policies and controls in the SDLC of the Denodo Platform to guarantee the product is delivered without known vulnerabilities.
   To protect our customers, those vulnerability reports are confidential and cannot be disclosed. Denodo provides security updates/notices to customers as a vulnerability affecting Denodo is found. Vulnerability reports summaries can be shared with our actual customers upon request.
2. **Medium Risk** - In the second level, we place the **Denodo Services** organization. Even when Denodo will not access/process/store customer's data, in the context of the resolution of a support case we could accidentally receive some sensitive information (e.g. in a log trace). Denodo's Support practices are based on industry-standard guidelines and best practices for the type of software/support marketed by Denodo.
3. **Low Risk** - In the third level, we place the whole **Denodo Organization**. To the extent that Denodo receives customer employee information during the ordinary course of doing business (such as through emails with Denodo personnel or through the company's websites). Denodo uses standard cybersecurity protection schemes to protect all such information complying with applicable laws in the same manner Denodo protects its own information and as the customer must also protect Denodo's employees' personal data.

In the context of a Vendor Risk Assessment, the goal is to evaluate the level of compliance of an organization, their policies, and corresponding controls, that applies to one or another of the aforementioned levels (i.e. 'Denodo Platform SDLC', 'Denodo Services' and 'Denodo Organization').

In the following sections we summarize at what level, in our understanding, should apply to those controls, asking evaluators to take that in mind when assessing Denodo's final score.

"DENODO PLATFORM SDLC"

- **Denodo Platform Development Security**: Secure code development and testing is deeply imbricated within the software development life cycle. Our technical product managers define the security guidelines that need to be

enforced in all the stages of development. Denodo runs static analysis of the code and vulnerability scanning in early development stages by using both Static and Dynamic Application Security Testing (SAST, DAST) tools such as Veracode, SonarQube and Error Prone, as well as internally developed security tests and code reviews (peer review by other developers). Tests are executed on every release and update, and all new code is automatically scanned by two different tools to find security vulnerabilities in early development stages. Also, penetration tests are run periodically and before each release using Veracode, one of the leading providers in that space. Active monitoring of vulnerabilities databases is also performed.

- **Denodo Platform Incident Management**: Denodo provides security updates/notices to customers as a vulnerability affecting the Denodo Platform software is found. Customers are notified through Denodo Support Site and, if needed, a hotfix solving the vulnerability is generated and made available for customers.

"DENODO SERVICES"

- **Denodo Services Security**: Denodo's Support practices are based on industry-standard guidelines and best practices for the type of software/support marketed by Denodo. Denodo maintains an ISO 27001:2022 certified set of ISMS documentation including risk management controls; the effectiveness of these policies and procedures are attested to under independent audit by qualified assessors to issue the ISO 27001:2022 certificate.

- **Denodo Suppliers Security**: Denodo relies on trusted providers to provide the Support Services and store the associated support data. All those providers own security certifications that we have included in the selection criteria.

"DENODO ORGANIZATION"

- **Information Security Policies**: Denodo has implemented and proactively maintains internal policies and processes to ensure it complies with all applicable data protection laws, and in particular with GDPR and Privacy Shield.

  Denodo continuously monitors applicable data protection and privacy regulations and guidelines. Denodo's legal team works with outside counsel in the jurisdictions where we conduct business to ensure that appropriate precautions are observed.

  To the extent that Denodo receives customer employee information during the ordinary course of doing business (such as through emails with Denodo personnel or Support services requests), Denodo uses industry best practice cybersecurity protection schemes to protect all such information complying with applicable laws, in the same manner Denodo protects its own information, and as the customer must also protect Denodo's employees personal data. Additionally, Denodo processes customers' data in compliance with the Supplier Data Processing Agreement (DPA) accessible at https://www.denodo.com/en/page/data-processing-agreement.

  Denodo respects the privacy of its customers, partners and other visitors to the company's websites and protects personal information in accordance with the Denodo Privacy Policy, available at https://www.denodo.com/en/privacy-policy, and other local regulations such as the California Consumer Privacy Act (CCPA), available at https://www.denodo.com/en/california-privacy-addendum .

  Denodo, as part of its Information Security Management System's (ISMS), and at least once a year, measures, reviews, documents and audits its compliance with ISO 27001:2022 IT Security obligations, officializing the

proactive approach towards security, and attesting the highest quality, rigor, and integrity of its solutions and services.

- **Information Security Management System (ISMS)**: As part of the ISMS implementation project, all policy procedures have been reviewed, including:
    - **Risk Management**: In order to improve the confidence our customers have in Denodo, a Risk Management System has been implemented within the scope of Denodo Information Security Management System (ISO 27001:2022 certified).
    - **Personnel & HR Security**: Denodo performs background screening to new hires. Denodo employees receive security awareness training as part of the on-boarding. Annual refresher training is also performed.
    - **Business Continuity**: Even when this is not required due the type of services Denodo provides, and in order to improve the confidence our customers have in us, a Business Continuity Management System has been implemented as part of the Denodo Information Security Management System (ISO 27001:2022 certified).

      Members of the Denodo Services teams are spread across Denodo's offices around the world (you can find the list of Denodo Support Centers at https://support.denodo.com). The distribution of our services personnel and the fact that our support services are mainly remote by web, email or phone; facilitates the continuity of Denodo's post sales services. In addition, Denodo does not operate the infrastructure where the Denodo Platform runs in our customers, and Denodo does not rely on 3rd-parties to deliver professional, educational nor product support services to our customers either. In summary, Denodo leverages the above strengths to ensure the continuity of Denodo business and to guarantee the delivery of our services at the standards set forth under SLAs.

      Denodo Security Policy and Business Continuity Policy are confidential information we do not disclose. Instead, you can find statements about both policies at: https://www.denodo.com/en/page/information-security-policy-statement , https://www.denodo.com/en/page/business-continuity-policy-statement

      In addition, the source code of the Denodo Platform (COTS solution Denodo markets) is stored in a third-party escrow provider at the disposal of our customers in the event of disaster.

DENODO ISO-27001 CERTIFICATION

In response to increasing security and compliance requirements from our clients and partners, Denodo got the ISO 27001:2022 certification in January 2024 officializing the proactive approach towards security and attests to the highest quality, rigor and integrity of its solutions and services.

Denodo Vendor Assessment - Interpretation Guidelines

A-LIGN

Denodo Technologies Inc.
Certificate Number: ISMS-DE-012624

CERTIFICATE OF REGISTRATION

Information Security Management System
ISO/IEC 27001:2022

Denodo Technologies Inc.

A-LIGN Compliance and Security, Inc. certifies that the organization operates an Information Security Management System that conforms to the requirements of ISO/IEC 27001:2022. The scope and boundaries of the ISMS is as follows:

The Information Security Management of the information systems that take part in the delivery of professional, education, support and IT Infrastructure & Data: services to Denodo Technologies customers on all the facilities.

Certificate	ISMS-DE-012624	**Original Certification Date**	January 26, 2024
Version	1.0	**Expiry Date**	January 26, 2027
Statement of Applicability	Version 3.1 (October 26, 2023)	**Issuance Date**	January 26, 2024

400 N Ashley Drive
Suite 1325
Tampa, FL 32602
888.702.5446
info@a-lign.com

A-LIGN.COM

Authorized by:

Stephanie Oyler
VP of Attestation Services