

ANNEX - DESCRIPTION OF SERVICES

I. LOBSTER DATA PLATFORM

1. General

The Lobster Data Platform is a powerful, no-code integration solution that can be used to configure, control and automate digital business processes. Seamless data integration between different systems, formats and applications is possible without any programming effort. Its modern, browser-based user interface allows users to develop, manage and monitor interfaces intuitively, particularly in the context of electronic data interchange (EDI) with business partners.

Configurations

Lobster Data Platform is licensed via Configuration Items. For integration, this includes all forms of data transformation (profiles and ETL pipelines). In orchestration, this includes user interface components (user-defined overviews, input forms and portals).

Application Connectors

Various application connectors are available for seamless integration with software solutions as a database source (JDBC), which enable data exchange via standard SQL. The special SAP connector enables connection to SAP systems via SAP ALE or RFC and the exchange of IDocs. Overview of application connectors:

- <https://www.lobster-world.com/en/marketplace/application-connectors/>

Lobster Data Platform

The Lobster Data Platform offers code-free data integration, combining process automation, data visualisation and data management in a single solution on a platform with various tools. The solution is a platform-independent system that is operated as a server. It is browser-based, allowing multiple users to work with the server at the same time. A database is connected to the platform, which serves as a repository for user data, developed profiles, etc. At its core, the platform is based on a clearly structured, six-step processing model: data is received, parsed, mapped, compared with databases, converted into target formats and then sent. The Lobster Data Platform supports a wide range of structured file formats and common communication protocols.

The focus is on the 'Automate & Visualise' approach: routine tasks such as converting, validating, routing or mapping data are fully automated. Each process step can be configured in a modular fashion, visualised graphically and monitored at any time – without any programming knowledge. The platform offers a multilingual user interface and supports transparent visualisation and traceability of all data flows. Fine-grained user, role and company management enables precise access control. At the data level, individual business objects can be modelled and managed, including status management, change tracking and a graphical editor. The possible applications range from classic supply chain management and shipping and procurement platforms to the control of internal processes, the creation of customer portals and tracking & tracing. Lobster Data Platform complies with current security standards: These include encrypted data transmission, role-based rights management, versionable configurations and comprehensive logging. With the server-side modules for DMZ and load balancing, highly

available, business-critical scenarios can be covered.

The complete range of services can be found in the online documentation:

<https://www.lobster-world.com/en/platform-documentation/>

2. LOBSTER DATA PLATFORM CLOUD (iPaaS)

The Lobster Cloud provides a standardised Integration Platform as a Service (iPaaS) designed specifically for business data integration. This comprehensive solution, built exclusively on the Amazon Web Services (AWS) infrastructure, combines performance, efficiency and standardisation in one package, enabling organisations to manage their data integration and business processes in a secure environment. The platform significantly reduces IT infrastructure complexity while ensuring scalability, security and performance with deployment options in Frankfurt (Germany) and Zurich (Switzerland). The cloud hosting solution described below is operated by Lobster Cloud Engineers. The Lobster Cloud uses only the reliable and high performance infrastructure in the following AWS regions:

Region	AWS-Description	Note
Germany - Frankfurt	eu-central-1	Standard region
Switzerland - Zurich	eu-central-2	Additional region

The service obligation assumed by Lobster includes the provision of the cloud infrastructure, remote managed services and the operation of the cloud infrastructure.

The Cloud Operation Services essentially include:

- Automated provisioning of the cloud infrastructure
- Controlled implementation of changes to the managed environment
- Providing a single point of contact (SPOC) to receive customer reported incidents, general service requests and/or change requests in the form of a 2nd level service desk.
- Root cause analysis for recurring incidents

Lobster Cloud Components

The Lobster Cloud uses the following core AWS components for a robust and secure infrastructure:

Web servers (EC2 instances):

- One EC2 instance per system component (DMZ, web server)
- Performance optimised for the respective package

Relational Database Service (RDS):

- A separate instance for test and production environment
- Amazon PostgreSQL RDS: Optimised for Lobster applications

Database with high availability:

- Amazon PostgreSQL Aurora cluster database with one read and one write instance

Firewall (Security Group):

- Dedicated security group for each web server and database

- Rule based access control
- Max. 960

Network (VPC):

- One Virtual Private Cloud per licence (contract) and customer
- Completely isolated network environment

Network and Security:

IP addresses:

- Fixed public IP address for each web server
- Variable internal IP addresses per web server and database

Security services:

- AWS GuardDuty: Intelligent threat detection
- AWS Security Hub: Centralised security management
- VPC run logs: Network monitoring (per web server)

Monitoring Options:

- Standard: 8/5 monitoring (supervised operation)
- Premium: 24/7 monitoring (supervised operation with 24/7 on-call alerting)
- Monitoring includes all web servers and database instances

A Lobster Cloud setup typically consists of a test and a production environment, which are automatically provisioned separately for each customer in a Virtual Private Cloud (VPC). Each test and production environment consists of an Amazon EC2 instance and an Amazon RDS database. Identical system sizes are selected for test and production systems. The following defined system sizes are available with AWS EC2 instance types based on Linux in combination with PostgreSQL database instance types via Amazon Relational Database Service (RDS):

System size	EC2 instance type	Server configuration	DB instance type	Database configuration
Entry	r6g.medium	8 GB RAM/1 vCPU/ 200 GB SSD	db.t3.medium	4 GB RAM/2 vCPU/ 100 GB SSD
Basic	t4g.large	8 GB RAM/2 vCPU/ 200 GB SSD	db.t3.large	4 GB RAM/2 vCPU/ 250 GB SSD
Standard	t4g.xlarge	16 GB RAM/4 vCPU/ 300 GB SSD	db.t3.xlarge	16 GB RAM/4 vCPU/ 250 GB SSD
Performance	t4g.2xlarge	32 GB RAM/8 vCPU/ 400 GB SSD	db.t3.2xlarge	32 GB RAM/8 vCPU/ 250 GB SSD

Test and production systems and associated DMZ instances are operated as a complete unit in the Lobster iPaaS Cloud.

The **Lobster Data Platform** offers the following main solutions in the Lobster Cloud:

- **Data World / Data Platform**
 - System size: Base Cloud Setup **Standard**
 - Upgrade to Performance possible
 - Additional DMZ (Basic system size) possible
 - Additional DEV environment (Basic system size) possible
 - Migration to High Availability (HA) possible
- **Data Platform Entry**
 - System size: Base Cloud Setup **Entry**
 - No size upgrades possible
 - No additional DMZ or DEV environment possible
 - Upgrade to 'Data Platform' possible
 - Migration to High Availability (HA) not possible

The Lobster Data Platform is accessed as usual via the browser. Direct access to the cloud resources, such as the Linux server or the database, is not possible. The customer does not have access to the Linux operating system or the shell.

Operating system

Status	Operating System	Support period
Current	Amazon Linux 2023 (or higher)	Current version

Database system

Status	Database-System	Support period
Standard	AWS RDS – PostgreSQL (16.x or higher)	Current version

If a system reboot is required, the customer can request this via a ticket. The following ports are enabled by default for the use of communication channels on the Lobster Data Platform:

80, 443, 9000

All other ports are closed by default. After consultation with the customer, additional ports can be opened for specific IP addresses.

2.1 Cloud Monitoring Service

All cloud systems are monitored 24/7 by a dedicated cloud monitoring tool. If faults are detected, Lobster automatically receives tickets and handles them in accordance with the contractually agreed Service Level Agreements (SLAs) - either during business hours (8/5) or around the clock (24/7).

Monitoring is carried out up to the application server based on a Java Virtual Machine (JVM). Lobster therefore monitors the systems (operating system, server, database and JVM) automatically in order to be able to react quickly. In the event of a fault, an alarm message is automatically sent to Lobster, which then independently initiates fault localisation and root

cause analysis for the system. Lobster is responsible for processing faults and recording error messages.

Prioritisation of incidents

All incidents are categorised and processed according to a priority system:

- **Emergency** - Critical system failures requiring immediate attention
- **High** - Significant issues affecting core functionality
- **Normal** - Standard issues with moderate impact
- **Low** - Minor issues with limited impact

2.2 Maintenance and patch management

The operating system of the Linux server is regularly maintained by Lobster. Patches are imported after technical evaluation by Lobster. The following policy applies:

1st Sunday of the month – Operating systems for all EC2 instances – between 06:00 and 8:00 UTC+1/+2

1st Sunday of the month – Lobster patching for test systems – between 08:00 and 09:00 UTC+1/+2

4th Sunday of the month – Lobster patching for production systems – between 06:00 and 07:00 UTC+1/+2

Every Monday – Database maintenance between 04:00 and 05:00 UTC+1/+2

The customer will normally be notified by email one week before each maintenance. If the customer has not provided their own email address for the maintenance email, it will be sent to the credentials address by default.

2.3 Backup and recovery of data

The backup of the EC2 instances and the databases for Test/Dev takes place daily between 02:00 and 03:00 UTC+1/+2 via AWS Backup. The databases for productive operation are backed up continuously. Backups are stored daily for 30 days for the productive infrastructure and for 7 days for the test/dev infrastructure.

The AWS Backup Vault and AWS Backup Vault Lock concept is used to provide an immutable backup policy. Restore from backup must be requested through support. The backup is used for disaster recovery. Disaster recovery will restore the EC2 instance or RDS database to the time of the last backup. It is not possible to determine the Recovery Point Objective (RPO) across the board, as it depends on the size and complexity of each individual system.

Other features:

- Monthly recovery tests with randomly selected customer systems on temporary infrastructure
- Compliance tests on temporary infrastructure
- Monitoring of executions
- Disaster Recovery Plan

3. OPTIONAL EXTENSIONS

3.1 Lobster DMZ

The Lobster DMZ in AWS serves as a critical security component that completely isolates the internal Lobster system from the public Internet. By providing a controlled access point while simultaneously shielding the internal Lobster system, network security is significantly

increased while ensuring the necessary connectivity for business processes. The DMZ is also known as a reverse proxy, as it fulfils similar functions: It receives requests from outside, forwards them in a controlled manner and returns responses, while completely hiding the internal systems. The DMZ acts as an authentication proxy and as a data buffer.

The DMZ has the following characteristics

- Acts as a publicly accessible endpoint
 - Allows internal system
- Provides security isolation:
 - Protects the internal Lobster system
 - Prevents direct external access to the internal Lobster system
- AWS- specific Security Groups
 - Uses dedicated AWS security groups for the DMZ
 - Enables granular control of inbound and outbound network traffic
 - Defines specific rules for supported protocols
- Centralised
 - Handles all traffic using standard protocols
 - SSH
 - FTP/SFTP
 - OFTP
 - AS2
 - HTTPS-Requests
- Data Buffering
 - Temporary storage of data when the internal system is unavailable
 - Ensures data continuity during maintenance or outages
 - Prevents data loss during connection problems
- Authentication Proxy
 - Forwards authentication requests securely to the internal Lobster system
 - Protects internal authentication mechanisms from direct external access
 - Enables single sign-on functionality without compromising security
- Data Validation
 - Checks incoming data for compliance with defined rules
 - Rejects data for which no appropriate processing channels exist
 - Reduces the risk of unexpected or non-compliant data entry

The system size of the DMZ can be selected independently of the base system. A Lobster DMZ is operated on one of the following EC2 instances with Linux:

Size	EC2 Instance type	Server configuration
Basic	t4g.large	8 GB RAM / 2 vCPU / 200 GB SSD
Standard	t4g.xlarge	16 GB RAM / 4 vCPU / 300 GB SSD

3.2 VPN

In order to connect systems and services in customer-owned on-premise data centres, private cloud environments or with another provider, a secure connection to the Lobster Integration Server can be established via a VPN. A site-to-site VPN connection is set up and operated exclusively via AWS Site2Site, i.e. via IPSec to the EC2 instances in the AWS Virtual Private Cloud (VPC). The technical requirements for setting up a site-to-site VPN connection via IPSec with AWS IPSec Site apply.

Mandatory requirements for the Customer gateway device for an AWS IPsec site-to-site VPN:

- Must support IKE (Internet Key Exchange), ideally IKEv2
- Must support IPSec
- Must be accessible via a static public IPv4 address
- Must support Dead Peer Detection

3.3 High-Availability-Standard

For the secure operation of critical data processing and production processes, a high-availability configuration can be set up as a standardised, robust infrastructure. Overall availability is increased by load balancing the requests across multiple servers, and Lobster Working Nodes as well as by the redundant design of all necessary components.

The Lobster High Availability (HA) configuration ensures that the Lobster Data Platform remains fully functional even in the event of a single server failure. This enterprise-grade deployment option has been specifically designed for organisations with the following requirements:

- Minimal downtime
- Increased fault tolerance
- Optimised performance in business-critical environments

This HA architecture effectively eliminates single points of failure and ensures system resilience through automatic failover mechanisms and intelligent load balancing.

A standard **Lobster Cloud High-Availability-Setup** consists of at least two Amazon EC2 instances in different AWS zones, an Amazon PostgreSQL Aurora cluster database in different AWS zones, a REDIS cluster with two EC2 instances in different AWS zones and a redundant Amazon Elastic File System (EFS).

Production setup:

2 DMZ Nodes, 1 Node Controller (NC), 1 Working Node (WN), REDIS Cluster, Elastic File Share, Cluster Database (DB)

System sizes and technical equipment:

- DMZ: Basic: 8 GB RAM, 2 vCPUs, 200 GB SSD
- NC/WN: Standard: 16 GB RAM, 4 vCPUs, 100 GB SSD
- EFS: 500 GB
- REDIS Cluster: 1,3 GB RAM, 2 vCPUs, 50 GB SSD
- DB: Cluster PostgreSQL Database: 16 GB RAM, 2 vCPUs, 150 GB SSD

Test setup:

1 DMZ Node, 1 Node Controller (NC), REDIS Cluster, Elastic File Share (EFS), Database (DB)

System sizes and technical equipment:

- DMZ: Basic: 8 GB RAM, 2 vCPUs, 200 GB SSD
- NC: Standard: 16 GB RAM, 4 vCPUs, 100 GB SSD
- EFS: 500 GB
- REDIS Cluster: 1,3 GB RAM, 2 vCPUs, 50 GB SSD
- DB: PostgreSQL Database: 16 GB RAM, 2 vCPUs, 150 GB SSD

3.4 DNS-Resolution

Redundant DNS resolvers for internal DNS resolution for VPN connections are optionally available, provided that a VPN via AWS Site2Site has been set up by Lobster.

DNS resolution is optimised, especially for scenarios with VPN connections to different cloud and on-premise resources. A redundant DNS resolver architecture is implemented for this purpose, which ensures stable, fast and fail-safe name resolution in the network.

II. LOBSTER DATA PRODUCTS

A **Lobster Data Product** is a fully managed service for standardised use cases that operates within the Lobster Data Network, hosted in the Lobster Cloud. It provides organisations with **plug-and-play integration** without the need for complex integration projects. The solution leverages Lobster's centrally **managed one-to-one** and **many-to-many integrations** within the Lobster Data Network. These enable seamless, asynchronous connectivity between business partners, systems and platforms. Thanks to **no-code technology**, only one connection per participant is required. This connection can then be used for all other participants. The product is particularly suitable for **recurring or highly standardised processes** such as supplier connections, invoice transmission or tracking information. All in all, Lobster offers a scalable, user-friendly and efficient solution for modern data integration.

The following Lobster Data Products are available:

- **Data Product Invoicing**
Invoice data including e-invoices, EDI and individualised invoices
- **Data Product Shipment**
Shipment data (including transport orders, acknowledgements, status updates)
- **Data Product Order**
Orders (purchase orders, acknowledgements, status updates)

Communication channels for Data Products

The following communication channels are available for all data products and are defined with the customer at the outset for both inbound and outbound transmissions:

a) **HTTPS**

One file is transferred per HTTPS call. Bulk or multiple transfers per HTTPS session are not possible. Several files can be transferred cyclically via HTTPS using multiple calls.

b) **AS2**

One file is transferred per AS2 call. Bulk or multiple sending per AS2 session is not possible. The transfer of multiple files via AS2 can be carried out cyclically via multiple calls.

c) **SFTP**

Multiple files can be transferred via an SFTP channel, which are processed asynchronously.

Data Product Invoicing

1. General

Lobster provides an e-invoice service to validate incoming invoices (inbound) from the client for e-invoice formats, create a readable visual copy in PDF format for each e-invoice, and deliver this to the client in an agreed target format and via an agreed communication channel.

For outgoing invoices (outbound) from the client, the e-invoice service creates an e-invoice format from an input format agreed with the client and forwards the e-invoice back to the client or forwards it to the business partner.

2. Validation of the e-invoice in the inbound process

Once the e-invoice is received, the data is validated against the underlying regulations and standards according to EN16931. The different e-invoice formats are automatically recognised. In addition, the e-invoices are validated against the latest versions of the official national regulations. The validators check whether the XML data conforms to the relevant standards with the specific rules and specifications in terms of syntax and semantics. For each e-invoice, the validators provide a return value for a basic decision ('OK' or 'ERROR') and which e- format it is. The validation result is returned to the client in JSON format as an attachment to the view copy for automated evaluation.

3. Visualise the e-invoice as a view copy in PDF format in Inbound

After receipt and successful validation, the transmitted e-invoice is generated as a view copy in a standardised layout as PDF/A-3 or as UBL. In the PDF version, the original transmitted e-invoice and the validation result are inserted as an attachment. In the UBL version, the transmitted original e-invoice, the validation result and also the view copy in PDF format are embedded separately as Base64. The view copies (PDF) are available in German and English for the general presentation and for the field labels. The language configuration is

centralised. The selected language is used for all ordered countries and e-invoices.

4. The customer remains fully responsible for the business content of the documents exchanged, including compliance with applicable laws, and for any resulting business obligations. E-invoices are available on the e-invoice platform for 30 days, after which they are deleted.

5. Communication channels

In addition to the general communication channels, the following communication channels are available for Data Product Invoicing:

a. E-Mail

E-Mail By default, e-mail is the standard communication channel that is used if no other is specified (backup communication protocol).

On the inbound side, a maximum of ten individual attachments (e-invoices) can be transmitted per e-mail in the inbound process. Only single-sort attachments of e-invoices (e.g. XRechnungen or ZUGFeRD invoices) can be processed per email. Compressed attachments (ZIP archive with e-invoices) cannot be processed. On the outbound side, a separate email is generated and returned for each incoming e-invoice in the inbound process. For each incoming e-invoice, an email is generated and returned containing the results of the validation as well as the view copy created for the respective e-invoice. The return value of the validation is specified in the subject of the email. This means that after receiving an e-mail with ten e-invoices, ten separate e-mails will be sent to the client with the respective validation results.

b. Peppol

Individual e-invoices are sent asynchronously via Peppol. The data format is Peppol BIS Billing V3 to ensure smooth and standardised communication across borders. To send and receive e-invoices, the customer must be registered in the Peppol e-Delivery Network via Lobster. One invoice is sent per call. It is not possible to send invoices in bulk or multiple times per session.

Lobster supports the following countries and their e-invoicing formats:

6. Germany

6.1 The following e-invoice formats are processed in the latest valid versions:

- a) XRechnung (UBL, CII) from version 3.0.2 (national standard for electronic invoices in Germany)
- b) ZUGFeRD as of version 2.3.2 (Factur-X, XRechnung) with CII
- c) Peppol BIS Billing V3

6.2 Receiving invoices (inbound)

Once successfully validated, a readable copy of the transmitted e-invoice is generated in a standardised layout as PDF/A-3. The transmitted e-invoice is embedded in this PDF as an attachment. A readable copy of a ZUGFeRD invoice is also generated despite a PDF already being available on the inbound side. The PDF component of a ZUGFeRD invoice can contain incorrect information; the embedded e-invoice (XML file) is legally binding. The XML file is

first validated and then processed into a readable PDF copy. The original ZUGFeRD file, the e-invoice (XML file) and the validation result are added as an attachment to the readable PDF copy that is created.

6.3 Sending invoices (outbound)

The source format of the customer's invoice data is converted into the requested e-invoice format for Germany in accordance with 6.1. If the ZUGFeRD e-invoice format is chosen, a readable PDF with the CII format is generated per e-invoice. If the Peppol communication channel is chosen, the Peppol BIS Billing V3 format is selected as standard.

7. Austria

7.1 The following e-invoice formats are processed in the latest valid versions:

- a) ebInterface from version 6.1
(national standard for electronic invoices in Austria)
- b) Peppol BIS Billing V3

7.2 Receiving invoices (inbound)

Once successfully validated, a readable copy of the transmitted e-invoice is generated in a standardised layout as PDF/A-3. The transmitted e-invoice is embedded in this PDF as an attachment.

7.3 Sending invoices (outbound)

The source format of the customer's invoice data is converted into the requested e-invoice format for Austria in accordance with 7.1. If the Peppol communication channel is chosen, the Peppol BIS Billing V3 format is selected as standard.

8. Denmark

8.1 The following e-invoice formats are processed in the latest valid versions:

- a) OIOUBL from version 2.1
(national standard for electronic invoices in Denmark)
- b) Peppol BIS Billing V3

8.2 Receiving invoices (inbound)

Once successfully validated, a readable copy of the transmitted e-invoice is generated in a standardised layout as PDF/A-3. The transmitted e-invoice is embedded in this PDF as an attachment.

8.3 Sending invoices (outbound)

The source format of the customer's invoice data is converted into the requested e-invoice format for Denmark in accordance with 8.1. If the Peppol communication channel is chosen, the Peppol BIS Billing V3 format is selected as standard.

9. France

9.1 The following e-invoice formats are processed in the latest valid versions:

- a) Factur-X from version 1.0.07
(national standard for electronic invoices in France)
- b) UN/CEFACT Cross Industry Invoice (CII)

- c) OASIS UBL from version 2.1
- d) Peppol BIS Billing V3

9.2 Receiving invoices (inbound)

Once successfully validated, a readable copy of the transmitted e-invoice is generated in a layout as PDF/A-3. The transmitted e-invoice is embedded in this PDF as an attachment. A readable copy of a Factur-X invoice is also generated despite a PDF already being available on the inbound side. A Factur-X invoice may contain incorrect information in the PDF component; the embedded e-invoice (XML file) is legally binding. An additional readable PDF copy, which is validated by the service, is therefore necessary. The original Factur-X file and the validation result are embedded as an attachment in the generated readable copy.

9.3 Sending invoices (outbound)

The source format of the customer's invoice data is converted into the requested e-invoice format for France in accordance with 9.1. If the Peppol communication channel is chosen, the Peppol BIS Billing V3 format is selected as standard.

10. Poland

10.1 The following e-invoice formats are processed in the latest valid versions:

- a) OASIS UBL from version 2.1
- b) Peppol BIS Billing V3

10.2 Receiving invoices (inbound)

Once successfully validated, a readable copy of the transmitted e-invoice is generated in a layout as PDF/A-3. The transmitted e-invoice is embedded in this PDF as an attachment.

10.3 Sending invoices (outbound)

The source format of the customer's invoice data is converted into the requested e-invoice format for Poland in accordance with 10.1. If the Peppol communication channel is chosen, the Peppol BIS Billing V3 format is selected as standard.

11. Belgium

11.1 The following e-invoice formats are processed in the latest valid versions:

- a) Peppol BIS Billing V3

11.2 Receiving invoices (inbound)

Once successfully validated, a readable copy of the transmitted e-invoice is generated in a layout as PDF/A-3. The transmitted e-invoice is embedded in this PDF as an attachment.

11.3 Sending invoices (outbound)

The source format of the customer's invoice data is converted into the requested e-invoice format for Luxembourg in accordance with 11.1. If the Peppol communication channel is chosen, the Peppol BIS Billing V3 format is selected as standard.

12. Luxembourg

12.1 The following e-invoice formats are processed in the latest valid versions:

- a) Peppol BIS Billing V3

12.2 Receiving invoices (inbound)

Once successfully validated, a readable copy of the transmitted e-invoice is generated in a standardised layout as PDF/A-3. The transmitted e-invoice is embedded in this PDF as an attachment.

12.3 Sending invoices (outbound)

The source format of the customer's invoice data is converted into the requested e-invoice format for Luxembourg in accordance with 12.1. If the Peppol communication channel is chosen, the Peppol BIS Billing V3 format is selected as standard.

13. The Netherlands

13.1 The following e-invoice formats are processed in the latest valid versions:

- a) Simplier Invoice UBL (SI-UBL) from version 2.0
- b) NL CIUS from version 1.0.3
- c) Peppol BIS Billing V3

13.2 Receiving invoices (inbound)

Once successfully validated, a readable copy of the transmitted e-invoice is generated in a layout as PDF/A-3. The transmitted e-invoice is embedded in this PDF as an attachment.

13.3 Sending invoices (outbound)

The source format of the customer's invoice data is converted into the requested e-invoice format for the Netherlands in accordance with 13.1. If the Peppol communication channel is chosen, the Peppol BIS Billing V3 format is selected as standard.

14. Peppol

- 14.1 Lobster is a certified Peppol Access Point Provider and offers companies connection to the worldwide Peppol network. Customers are registered by Lobster in the Open Peppol Network. Access to the Lobster Peppol Access Point for automated invoice processing is via a RESTful API, which enables customers to send and receive e-invoices.
- 14.2 Individual e-invoices are transmitted asynchronously via Peppol. The data format is always Peppol BIS Billing V3 in order to ensure smooth and standardised communication across borders. In order to send and receive e-invoices, the customer must be registered in the Peppol e-Delivery Network via Lobster.
- 14.3 Lobster, as a Peppol Service Provider, is authorised to provide the relevant Peppol services, including the receipt and/or transmission of Peppol business documents, on behalf of or for the benefit of the customer.
- 14.4 The Customer shall remain fully responsible for the business content of the exchanged documents, including their compliance with applicable law, as well as for any business obligations resulting therefrom.
- 14.5 Peppol is a network infrastructure with a set of agreements and standards for the transport of electronic documents. The network is managed by Open Peppol and the Peppol authorities of the participating countries.
Customers will be blocked from the Peppol e-Delivery Network if fraud, spam or other criminal activities are detected on behalf of the customer.

Data Product Shipment

Data Product Shipment is a digital service provided by Lobster for exchanging transport orders between shippers and freight forwarders. The shipper transmits transport orders electronically to the carrier, who in turn can confirm, reject or label them. In the further process, the freight forwarder sends status messages and tracking data on the progress of the consignment back to the shipper. Both parties also have the option of exchanging supplementary documents in Base64 format. Communication takes place via defined channels and in agreed data formats.

Data Product Shipment comprises various specialised transactions, including transport order, acknowledgement, status update, prealert, consolidation and cancellation. Other functions include bookings (batch, container), import and export documents, warehouse status, ground handling instructions and anonymous tracking based on a loading or transport list. Data Product Shipment thus enables data integration for comprehensive, transparent and automated control and monitoring of logistics processes along the entire transport chain.

Data Product Order

Data Product Order is a standardized Lobster data product designed for the digital exchange and management of purchase orders between business partners. It enables end-to-end electronic exchange of purchase orders, acknowledgements, and status updates via predefined communication channels and formats. The buyer submits a purchase order electronically to the supplier, who can then accept, decline, or acknowledge the order with optional comments. Any updates or changes to the order can also be transmitted automatically.

The scope of services includes the following transactions: sending and receiving orders (Order, Purchase Order), accepting orders (Accept), acknowledging orders (Acknowledgement), declining orders (Decline) and updating orders (Update). The product ensures efficient, asynchronous communication between purchasers and suppliers without media discontinuity and significantly reduces manual effort and sources of error. Data Product Order is particularly suited to recurring procurement processes where speed, visibility and automation are critical.

Orders can in turn lead to shipments. In this way, Data Product Order can work closely with Data Product Shipment.

Lobster DATA GmbH

Bräuhausstraße 1
D-82327 Tutzing
T: +49 8158 4529 300
information@lobster.de