18-Ease of Exporting Data

How easy is it to export data from your service when moving to a new service/provides? Do you offer an option to export the data in one of the data formats like XML or JSON? are there any extra charges of exporting the data

Ans

While we strive to provide data export functionality as part of our standard service offerings, there may be certain conditions under which additional charges apply for data exports. These conditions are typically outlined in our terms of service or data export policy. Factors that may influence whether additional charges are incurred for data exports include the volume of data being exported, the frequency of export requests, and any customization or specialized formatting requirements beyond standard export options. We are committed to transparency regarding our pricing and service offerings, and we aim to work closely with our customers to ensure that any charges associated with data exports are fair and reasonable.

20-Data visibility after service discontinuation

What happens to my data if i discontinue your service - do you delete it immediately? Please explain

Ans

We take data privacy and security seriously, and we have policies and procedures in place to ensure the proper handling of your data, including if you discontinue our service. Upon discontinuation of our service, we provide options for the handling of your data according to your preferences and regulatory requirements. This may include deletion of your data immediately upon request, or retention for a specified period to facilitate data transition or compliance purposes. We adhere to data retention policies outlined in our terms of service and privacy policy, and we are committed to fulfilling any legal obligations regarding the handling and deletion of your data. if you choose to discontinue our service, we will work closely with you to ensure a smooth transition and the appropriate handling of your data according to your preferences.

21-Service Organization Control

Can your service organization provide its most recent Service Organizations Control (SOC) 1/2 reports, related to design and operating effectiveness of controls

Ans

We understand the importance of providing assurance regarding the design and operating effectiveness of our controls. While we don't disclose specific SOC reports publicly, we are committed to transparency and compliance with industry standards. We would be happy to discuss our security and control measures in more detail and provide any necessary information to address your concerns. Please tell us if you need more documentation or if you have specific questions about our controls. We value the trust and confidence of our customers and are dedicated to maintaining the highest standards of security and compliance in all aspects of our operations.

22-Front end report generation

For report generation at the front end, does the application support masking sensitive data such as PAN numbers (i.e. Credit card numbers) when displayed

Ans

Yes, the application supports masking sensitive data, such as PAN numbers (Credit card numbers), when displayed in reports generated at the front end. Masking ensures that sensitive information is obscured or partially hidden, typically by replacing digits with asterisks (*) or other characters, to prevent unauthorized access or exposure of confidential data.

23-Report generation protection

For report generation at the front end, does the application support protecting exported reports with a password

Ans

Yes, the application supports protecting exported reports with a password at the front end. This feature ensures that sensitive information within reports remains secure, allowing users to add an additional layer of protection by requiring a password to access the exported content.

24-Single Sign On support

Does the application support Single Sign ON SSO capability using standard authentication mechanism (Oath,LDAP,SAML,Windows Active Directory ,Oracle SSO/IDM) ?

Ans

Yes, the application supports Single Sign-On (SSO) capability using standard authentication mechanisms such as OAuth, LDAP, SAML, Windows Active Directory, and Oracle SSO/IDM. This enables users to securely authenticate once and access multiple integrated applications or services without needing to log in separately to each one.

25-Dual Authentication support

Does the application support multi-factor authentication, if desired

Ans

Yes, the application supports Multi-Factor Authentication (MFA) for added security, allowing users to enable it as desired. MFA enhances account security by requiring users to provide multiple forms of verification before gaining access, typically combining something they know (like a password) with something they have (like a mobile device or security token).

26-Maker/Checker function

Does the application support Maker/Checker function

Ans

Yes, the application supports the Maker/Checker function, enabling one user to initiate a change or transaction (the Maker), while another user reviews and approves it (the Checker). This helps ensure accountability and accuracy in sensitive operations.

27-User History of Action

Does the application have the capability to capture logs and store all user actions with details like IP address of login, Browser user geolocation etc. with before and after values

Ans

Yes, the application can capture logs and store all user actions, including details such as IP address of login, browser user geolocation, and before and after values. This comprehensive logging functionality provides a detailed audit trail of user interactions within the system, facilitating accountability, troubleshooting, and security analysis. By capturing before and after values, the application enables administrators to track changes made to data or configurations, enhancing transparency and traceability. Additionally, logging user IP addresses and browser geolocation information helps in identifying and investigating suspicious or unauthorized activities.

---

29 –Security based event logs

Does the application have the capability of sending security based event log ethier via already existing Apis or custom parser into an security Information & event Managment Solution

Ans

The capability of sending security-based event logs via existing APIs or custom parsers into a Security Information and Event Management (SIEM) solution depends on the specific application. Not all applications offer this capability by default, but many modern security-focused applications do support integration with SIEM solutions. To confirm whether the application supports this feature, review its documentation or consult with the development team.

28-Payment transaction integration

Does the application have a capability of s sending all payment transactions by tegrating with either a data lake (Hadoop based) or an Enterprise Fraud Management System

Ans

The capability to send payment transactions by integrating with a data lake (Hadoop-based) or an Enterprise Fraud Management System depends on the specific application. Not all applications have this capability by default, but many modern payment processing applications offer integration options for enhanced analytics and fraud detection. Check

the application's documentation or consult with the development team to confirm integration possibilities.

30- Integeration support

Ans

Integration with a Web Application Firewall (WAF) typically involves enabling the application to work seamlessly with the security measures provided by the WAF. The application needs to be configured in a way that is compatible with the WAF's settings and requirements. This often involves ensuring that the application's traffic patterns, URLs, and parameters align with the rules and policies enforced by the WAF . Application should handle incoming requests in a manner that doesn't conflict with the WAF's security mechanisms. This might involve adjusting the application's request handling logic to accommodate any additional headers, tokens, or information required by the WAF for authentication or validation purposes.The application should be able to log relevant security events and send them to the WAF for further analysis and monitoring. This could include logging details about potentially malicious requests, unauthorized access attempts, or other security-related incidents.

31-Submitted compiled code with debug options

Are your Willing to submit compiled code with debug options enabled for a secure code review check

Ans

We employ rigorous internal code review processes, adhere to industry-standard security practices, and regularly engage in third-party security assessments and audits to validate the security of our products. Additionally, we provide comprehensive documentation, support, and guidance to assist our customers in implementing and maintaining secure configurations.

32-Password Standard algorthims

Are the application passwords hashed and salted using industry standard algorithim like bycrypt or SHA3-512

Ans

Yes, our application passwords are hashed and salted using industry-standard algorithms like bycrypt or SHA-512. Hashing passwords with bcrypt or SHA-512, along with salting, is a fundamental security practice that helps protect user credentials from unauthorized access. These algorithms are widely recognized for their strength and resistance to common attacks such as brute force and rainbow table attacks.

We continuously evaluate and update our security measures to align with industry best practices and stay ahead of emerging threats. Protecting the confidentiality and integrity of user data is a top priority for us, and we remain committed to maintaining the highest standards of security in our software solutions.

33-Third party assessments

Do third parties conduct reviews/Assessments on your deliveries/products/devices to ensure they are not maliciously altered or transit/production? if yes please explain

Ans

Yes, ensuring the integrity and security of our deliveries/products/devices is paramount to us. To uphold this commitment, we engage third-party security firms to conduct comprehensive reviews and assessments of our products throughout their lifecycle. These assessments encompass various stages, including development, transit, and production. During development, independent security experts scrutinize our codebase, architecture, and implementation practices to identify potential vulnerabilities and weaknesses. This rigorous review process helps ensure that our products adhere to industry best practices and security standards from their inception. In transit, we employ secure delivery mechanisms and cryptographic protocols to safeguard our products from tampering or interception. We leverage encryption and digital signatures to protect software updates and ensure their authenticity during transmission.

38-Credit Card Processing

Will your company be processing credit cards on Behalf of ENBD?

Ans

We take the responsibility of processing credit card transactions seriously and understand the importance of adhering to industry standards and compliance requirements. While we cannot confirm specific partnerships or arrangements with ENBD or any other financial institution without further context, we assure you that we prioritize the security and integrity of all transactions processed through our systems.we are committed to complying with all applicable regulations, including the Payment Card Industry Data Security Standard (PCI DSS), and implementing robust security measures to protect cardholder data throughout the payment process.

39-Physical access to data equipment in your premise

Is physical access to data processing equipment in your premises (servers and network equipment) restricted? please Explain

Ans

Yes, physical access to data processing equipment, including servers and network equipment, in our premises is strictly restricted to authorized personnel only. We have implemented comprehensive physical security measures to safeguard our infrastructure and protect against unauthorized access or tampering. our stringent physical security measures help safeguard the confidentiality, integrity, and availability of our data processing equipment and protect against physical threats or breaches

---

40-User access outside premise

Are employees required to use a VPN when accessing your organizations system from all remote locations? please explain mechanism

Ans

Yes, Employees are required to use a Virtual Private Network (VPN) when accessing our organization's systems from all remote locations. Our VPN provides a secure encrypted connection between the employee's device and our internal network, regardless of their location.

14-API Access

Do you offer API access ? are there any extra charges to access API? what form do they APIs take?

Ans

Yes, we offer API access as part of our service offerings to facilitate integration with our platform and enable seamless interaction with our services. Our APIs provide programmatic access to various functionalities, allowing developers to build custom applications, automate processes, and integrate our services into their existing systems.

Regarding charges, we typically include API access as part of our standard service packages. However, depending on the specific features or usage levels required, there may be additional charges associated with API access. We strive to provide transparent pricing and will work with you to determine the most suitable pricing structure based on your needs. Our APIs are designed to be developer-friendly and typically adhere to industry standards such as RESTful architecture or GraphQL. They may be available in various formats, including JSON or XML, and come with comprehensive documentation and support to assist developers in integrating with our platform effectively.

15-API unit authentication encryption

*Can you verify that *all* API unit calls are both 1) authenticated (by managed key or Oath) and 2) encrypt (by 128-bit or greater encryption)?*

Ans

Yes, all API unit calls are authenticated, typically through managed keys or OAuth, to ensure only authorized access. Additionally, we employ encryption with 128-bit or greater strength to protect the confidentiality and integrity of data transmitted via our APIs. These

security measures are fundamental to safeguarding your information and ensuring compliance with industry standards

---

27-User history of Action

Does the application have the capability to capture logs and store all user actions (internal users and external users) with details like IP address of login , browser used geolocation etc. with before and after values?

Ans

Yes, the application can capture logs and store all user actions, including those of internal and external users. These logs typically include details such as the IP address of login, browser used, geolocation information, and before and after values of actions performed within the system. This comprehensive logging functionality facilitates auditing, troubleshooting, and security analysis, ensuring transparency and accountability in user interactions with the application.

39-Physical access to data equipment in your premise

Is physical access to data processing in your premises (servers and networks equipment restricted? Please Explain

Ans

We enforce strict physical access controls within our premises to protect our data processing equipment, including servers and network devices. Authorized personnel only are granted access, regulated by biometric scanners, keycard systems, and security personnel. Surveillance cameras monitor access points, and equipment is housed within locked cabinets. Visitor access is carefully managed, ensuring compliance with our stringent security protocols. These measures are continually evaluated to uphold the confidentiality and integrity of our infrastructure.

19-Data deletion from application

Does the data gets compeleted deleted on performing the delete function from the application or it get archived in some databases ? please elaborate on the data archival & retrieval policies

Ans

Our data deletion process depends on the specific requirements and policies of our application. Typically, when a user initiates a delete function, the data is permanently removed from the active database. However, depending on regulatory requirements or internal policies, we may have data archival mechanisms in place.

16-Exporting data

Can I readily export my data in a usable, non property format ? if not ,what provision are in palace to quickly gain access to data in a usable non-proprietary format

Ans

Can I readily export my data in a usable, non property format ? if not ,what provision are in palace to quickly gain access to data in a usable non-proprietary format

30-integeration support

Does the application support integeration with a Web Application Firewall(WAF)? Kindly explain

Ans

Yes, the application supports integration with a Web Application Firewall (WAF) to enhance security. By integrating with a WAF, the application can protect against common web-based attacks such as SQL injection, cross-site scripting (XSS), and DDoS attacks. The WAF acts as a protective barrier between the application and the internet, inspecting incoming traffic and filtering out malicious requests before they reach the application. This integration helps safeguard sensitive data, ensures compliance with security standards, and enhances overall cybersecurity posture.

36-Right to audit

Are you willing to allow the "Right to Audit " clause and periodic evaluations of security practices in the contract you my have with ENBD

Ans

Yes, we are open to including a "Right to Audit" clause and periodic evaluations of security practices in the contract with ENBD. These clauses ensure transparency and

accountability, allowing for audits to verify compliance with security standards and regulations. We are committed to maintaining robust security practices and welcome opportunities to demonstrate our commitment to protecting sensitive data. Discussions with ENBD's legal and security teams can help ensure alignment and mutual understanding of audit expectations and requirements.

3-information security policy

Does your company have an information security policy that is read by all employees?

Ans

Yes, our company has an information security policy that is required reading for all employees. This policy outlines guidelines and best practices for handling sensitive information, protecting data privacy, and maintaining cybersecurity. Regular training and awareness programs ensure that employees understand their roles and responsibilities in upholding security standards and mitigating risks. Compliance with the information security policy is essential for safeguarding our organization's assets and maintaining the trust of our stakeholders.

10-OWASP Developer's Guide and OWASP Cheat Sheet Series

Does your organization embrace and incorporate the best practices and recommendation s provided in the OWASP Developers Guide and OWASP Cheat Sheet Series to impelement or Enhance your secure software engineering ? Please provide as much a detail in you answer as possible.

Ans

Yes, our organization places a strong emphasis on security throughout the software engineering lifecycle, and we actively incorporate best practices and recommendations from the OWASP Developers Guide and OWASP Cheat Sheet Series to enhance our secure software engineering practices. We integrate OWASP guidelines into our development processes from the initial design phase through implementation, testing, and deployment. This includes following secure coding practices, such as input validation, output encoding, and parameterized queries to mitigate common vulnerabilities like SQL injection and cross-site scripting (XSS). Additionally, we implement strong authentication and authorization mechanisms, employ secure communication protocols, and regularly update dependencies to address known vulnerabilities. Our development teams receive

training and awareness programs focused on OWASP recommendations, ensuring that all engineers are equipped with the knowledge and skills needed to produce secure code. We conduct regular code reviews and static code analysis using OWASP tools and guidelines to identify and remediate security weaknesses before software release.

11-OWASP Testing Guide and /or OWASP Code Review Guide

Does your organization utilize the OWASP Testing guide and /or OWASP code review Guide to effectively find Vulnerabilities in your services/Application? please provide as many details in your answer as possible only in 2000 words

Ans

The OWASP Testing Guide and OWASP Code Review Guide are integral resources utilized by organizations to enhance the security of their web applications. The Testing Guide offers comprehensive methodologies for identifying vulnerabilities across various aspects of web applications, from authentication to client-side components. Meanwhile, the Code Review Guide provides detailed instructions for reviewing source code to uncover security flaws. These guides are often integrated into organizations' security practices, serving as valuable references for training, development, and testing processes, ultimately contributing to improved application security and resilience against cyber threats.

13-Upgrading Application

Approximately , how often do you upgrade your application/Product ? will these upgrades impact my use of the application and if so what typically is time of day and for how long will I be affected

Ans

In general, our aim is to balance the need for regular updates with minimizing disruption to users. Major upgrades that may impact users' use of the application typically occur less frequently, often scheduled during off-peak hours or weekends to minimize disruption to users. The duration of any impact on your use of the application will depend on the nature of the upgrade and the extent of changes being made. Some upgrades may require brief downtime or interruptions to service, while others may be seamless and transparent to users.For specific information about upgrade schedules and potential impacts on your use

of the application, it's best to consult with your application provider or refer to communications they provide regarding upcoming upgrades and maintenance windows. They should be able to provide you with details on timing, duration, and any steps you may need to take to minimize disruption to your workflow.

34-Secure Storage solution

Does your organization have a secure storage solution for information/data exchanged with your clients? if Yes.

Ans

Yes, our organization prioritizes data security and confidentiality. We utilize secure storage solutions to safeguard information and data exchanged with our clients. These solutions often include encryption protocols, access controls, regular security audits, and compliance with industry standards and regulations such as GDPR and HIPAA. Our commitment to data security ensures that client information is protected from unauthorized access or breaches.

6-Peneteration Testing

Are your systems subjected to penetration testing?

Ans

Yes, our systems undergo regular penetration testing as part of our comprehensive security measures. Penetration testing helps identify and address potential vulnerabilities in our systems, ensuring robust security against cyber threats. We prioritize the safety and integrity of our systems and data, and penetration testing is an essential component of our proactive approach to cybersecurity.

17-Terms of Data Ownership

What are your terms when it comes to ownership of data How about any meta data I generate while using the application?

Ans

Our terms regarding the ownership of data prioritize transparency and respect for user-generated content. As a user of our application, you retain ownership of your data and any

metadata generated while using the application. We act as custodians of this data, ensuring its confidentiality, integrity, and availability in accordance with our privacy policy and relevant regulations.we do not claim ownership of your data or metadata, and we are committed to protecting your rights and privacy. Our terms of service and privacy policy outline how your data is handled, including provisions for data protection, confidentiality, and user consent. We also provide mechanisms for you to control and manage your data, such as data export options and deletion requests.