SEON

Businesses' first line of defense
against online fraud

End-to-end
fraud prevention & AML

Privacy & Security Whitepaper

Table of Contents

1. Introduction

The battle against digital fraud has become a critical mission for businesses worldwide in an increasingly interconnected digital landscape. At SEON, we understand the profound impact of fraud on your operations, reputation and customers. That's why we are committed to delivering innovative, effective and secure tools that empower businesses to detect and prevent fraud by providing comprehensive information about the online platform user.

Our mission: empowering businesses, safeguarding data

SEON is a Software-as-a-Service (SaaS) company that provides a cloud-based machine learning platform to combat digital fraud. Our services are meticulously designed to equip organizations with the tools they need to detect, prevent and mitigate fraud, all while preserving the privacy and security of individuals' data.

Understanding seon's services

SEON's platform provides inputs for user profiling decisions on the transaction level by performing real-time inquiries from public databases and collecting publicly available information from social media providers based on individual API calls made by our customers, leveraging and enriching the personal data they submit to SEON. Furthermore, if enabled, our Device Fingerprint tool can collect thorough insight about the devices associated with a user. In this way, SEON can deliver comprehensive information about our customer's users by providing a completely transparent decision and fraud score as a response, allowing for quick and accurate fraud detection and user verification. SEON's algorithm is based on industry and geography-specific pre-added rules, our customers' custom rules and machine-learning rule suggestions.

Along with the social media, digital and device footprint solution, an essential part of the SEON service is our AML API, which allows our customers to complement their fraud prevention toolkit with anti-money laundering tools to assist them in complying with their obligations concerning the Sixth Anti-Money Laundering Directive (EU) 2018/1673 (AMLD6), as well as the sanction measures issued by the United Nations Security Council. This tool, which may be used as a part of our Fraud API integration, a standalone API, or through the SEON Admin Panel, allows our customers to pair the data unearthed by SEON's data enrichment tools with PEP, sanctions and high-risk names to counter financial crime all in one place using SEON. However, please note that SEON does not guarantee that using our solution will result in complete compliance with AMLD 6.

In summary, SEON is tailored to meet the present needs by offering an easy-to-integrate, easy-to-use, modular tool that is usable in any industry but can be customized to fit industry-specific needs.

For more information about our product, please visit SEON's Documentation Page.

Our dedication

In the digital age, trust and privacy are more critical than ever. At SEON, our success depends on your confidence in our ability to safeguard your data. This whitepaper demonstrates our unwavering commitment to transparency, compliance with data protection regulations and responsible data handling practice, where we will provide a comprehensive overview of how SEON collects, processes and stores data within the scope of our services and of our implemented security measures. We will delve into the specific measures we have put in place to protect personal data and the individual's rights and choices concerning the personal information we handle. Furthermore, we will highlight our commitment to compliance with relevant data protection regulations, including the General Data Protection Regulation (GDPR), the United Kingdom General Data Protection Regulation (UK GDPR) and the California Consumer Privacy Act (CCPA)/California Privacy Rights Act (CPRA)[1], and outline our procedures for handling data breaches.

Thank you for choosing SEON as your trusted partner in the ongoing battle against digital fraud. Together, we can navigate the digital landscape securely and confidently, knowing that the data remains protected and your business is safeguarded.

2. Core principles

Our privacy compliance posture is designed following the ISO 27001 and SOC 2 Type 2 standards.

Privacy-by-design

We implement the privacy-by-design approach throughout SEON's Software Development Lifecycle to stay compliant with relevant privacy requirements on

- Lawfulness, fairness and transparency,
- Purpose limitation,
- Data minimization,
- Accuracy,
- Storage limitation,
- Integrity and confidentiality,
- Accountability.

Assessments and reviews

We conduct annual security and privacy threat modeling, create detailed engineering architecture plans focusing on privacy engineering and perform security assessments and privacy reviews before and after new feature releases. We repeat these assessments and reviews annually to monitor these aspects continuously.

Data chain

We take vendor security for sub-processors included in SEON's data chain thoughtfully. SEON's vendor management framework provides a solid basis for conducting combined security, privacy and legal assessment (due diligence) upon engaging with a new vendor. This means that SEON exclusively partners with reliable sub-processors who are held to security standards at least as rigorous as our own. We make every effort to engage only those sub-processors who are essential to our operations.

Data retention and erasure

[1] SEON's Information Security Management System and Privacy Framework are CCPA/CPRA compliant (GDPR and CCPA/CPRA are fairly consistent), however CCPA applies to organizations that collect personal information from more than 50,000 CA consumers, and CPRA applies to organizations that collect data from more than 100,000 CA consumers and SEON's operation (number of transactions) does not meet these figures. For details on how SEON complies with CCPA/CPRA, please request our "CCPA - GDPR Cross-Compliance Matrix" from your SEON sales contact or account manager.

SEON's data erasure processes and retention periods are in accordance with SEON's commitments, which are included in the Data Processing Agreement and available on SEON's website. Customers can also delete their data through the Erase API endpoint or from the Admin Panel UI.

Continuous monitoring and consultancy

Our dedicated compliance and security teams continually monitor SEON's privacy and security compliance status. This involves annual internal and external audits to identify risks and gaps. Identified gaps are discussed during regular consultancy meetings and addressed on time.

Operational practices

A range of security controls are designed to address SEON's systems' security criteria. Such security controls include permitting and restricting system users' access to personal data and the information they need based on their roles and responsibilities while prohibiting them from accessing information not required for their role. Policy and technical measures strictly restrict the number of employees with access to production data to the absolute minimum.

Product security

SEON has implemented various security controls to keep its systems and personal data safe. These include using encryption technologies to protect customer data at rest and in transit and formal processes to grant and revoke access to personal data.

Reliability, scalability & availability

Hosting data with SEON's cloud-hosting partners while focusing on product resiliency to minimize downtime and optimize performance with redundancy and failover options globally while maintaining multiple locations and availability zones across the region. The utilized technology allows a five-minute point-in-time recovery in case of a data loss incident.

Security processes

A range of vulnerability management and security processes to detect security and vulnerability issues allows SEON to address identified gaps as soon as possible to minimize the impact.

Development security

Measures to include the security aspect from the beginning and throughout the entire development process. This includes the involvement of security professionals during the design phase, in the testing and post-go-live monitoring, and various automated security tools and secure development-related guidelines.

Audit assurance

Our internal control system is audited by an independent third party on a yearly basis.

3. Seon's privacy & security scheme

3.1 Our roles

SEON as a data controller

For individuals using our services, contact persons of our customers when negotiating contracts, visitors to our website, social media sites, webinar participants or any other persons interacting with us directly, our Privacy Policy outlines our commitments as data controllers to safeguard these individuals' privacy and provide details on the collection, use and management of their personal data. SEON's role as a data controller extends to instances where individuals apply for positions at SEON. The processing of such data is governed by our Recruitment Privacy Notice.

SEON as a data processor

In the case of our customers' users (our customers are the online service providers using our services), our customers assume the role of the data controller for their users' personal data shared with SEON in connection with their use of our services. In this case, they, as data controllers, determine the purposes and means of processing personal data, while SEON acts as the data processor, processing data on our customer's behalf. In this scope, our Data Processing Agreement encompasses the commitments concerning data processing and the international transfer of data, if applicable.

Considering that this whitepaper is essentially dedicated to You as our customer or potential customer as a source of information, in the following, we will primarily focus on the relationship between You acting as data controller and SEON acting as data processor and our obligations and commitments regarding Your data.

3.2 How SEON meets the Privacy-by-Design approach

Principle	SEON's measures
Lawfulness, fairness and transparency	The legal basis for the processing of personal data by SEON as a data processor is the performance of a contract: the subscription agreement concluded between SEON and our customers which governs the fraud prevention services provided by SEON. However, the lawfulness (including having an appropriate legal basis), fairness and transparency for the entirety of the processing lies with our customers as data controllers. Our practical experience shows that the following legal bases are the most common for our customers for the processing of the customers' data: ● legitimate interest (prevention of fraud) or sometimes consent, if applicable. ● in case of financial institutions, fulfillment of a legal obligation to follow the PSD2 and the implementation of national laws or other similar legislation. ● fulfillment of a contract in which the data subject is one of the parties, or it is necessary to take steps at the request of the data subject prior to the conclusion of the contract (the data subject uses a service whose element is the fraud prevention function); ● when using the AML API, the fulfillment of a legal obligation to be in compliance with strong or soft Know Your Customer (KYC) requirements.
Purpose limitation	This requirement is also essentially our customers' as data controllers obligation to meet. SEON, operating as a data processor, conducts its data processing activities exclusively to create and manage the accounts of its users, provide the SEON services to our customers as data controllers and negotiate its contracts. These services are aimed at aiding our customers in identifying and preventing fraudulent transactions, ultimately minimizing the potential harm and damages caused by fraud. Moreover, we aim to enhance KYC transparency and, more broadly, contribute to the establishment of a secure digital economy. It is important to highlight that we refrain from constructing databases from the data we handle, thus we don't process customer data for our own purposes and any data that is no longer in use is promptly deleted.

Data minimization	SEON processes data that is strictly necessary and pertinent to deliver our services. It's crucial to emphasize that our customers have the autonomy to select the data upon which our services shall rely. Hence, scope of the data processed by SEON is determined and controlled by our customers.
Accuracy	The SEON service is real-time, and it provides feedback to our customers based on accurate, up-to-date data. In instances where our customers opt to restart a transaction, we consistently present the most recent data available.
Storage limitation	By default, customer data is stored for 1 year by SEON unless our customer instructs us otherwise.
Integrity and confidentiality	We apply strict technical and organizational measures to ensure the integrity and confidentiality of the data processed by us, in accordance with ISO 27001 and SOC 2 Type 2 standards. This includes, inter alia, that access to data is restricted only to the authorized individuals based on least-privilege principle.
Accountability	As a data processor, we put our reasonable efforts into supporting the data controller in compliance with data protection legislations. To achieve this, we steadfastly adhere to the highest bar principle.

3.3 Privacy & Security Personnel

Our Compliance Team

SEON has a dedicated Compliance Team deeply committed to upholding SEON’s Privacy Scheme and handling all kinds of privacy-related matters concerning the data of our valued customers, employees, and all those who entrust their data to us. Our Compliance Team collaborates closely with our Security Team to ensure that our privacy and security efforts are harmonized, guaranteeing the safety of personal data.

SEON’s Compliance Team is responsible for

- Driving compliance (including privacy compliance) efforts and coordinating relevant projects within SEON;
- Integrating privacy & security compliance best practices and baselines into the processes, tooling, and default configurations used throughout the SEON organization;
- Building up and maintaining SEON’s internal compliance control system (based on ISO 27001 and SOC2/COSO);

- Conducting/contributing to internal and external audits;
- Helping with regulatory compliance-related (security, privacy, legal) questions or issues; and
- Assisting in product development from a compliance/regulatory perspective.

Our Data Protection Officer is leading our privacy efforts, tasked with converting regulatory knowledge into practical enhancements to reinforce our commitment to data privacy. Our Data Protection Officer also serves as the primary point of contact for supervisory authorities and customers with any privacy compliance queries.

If you have any privacy compliance inquiries, you may contact the team at compliance@seon.io and/or our Data Protection Officer at dpo@seon.com.

Our Security Team

SEON's Security team is responsible for designing, executing, managing, and assessing SEON's security and privacy controls, policies, standards, baselines, procedures, and guidelines.

The Information Security team is entrusted with a spectrum of precise responsibilities, including

- Security Management: Managing the day-to-day security operations, which includes incident response, access control, and identity management;
- Privacy Compliance: Ensuring adherence to data protection regulations and facilitating regular audits to guarantee data privacy and compliance;
- Risk Assessment: Conducting regular risk assessments to identify potential vulnerabilities and developing strategies to mitigate them;
- Procedure Development: Crafting detailed security procedures and guidelines for employees to follow in various scenarios, such as data breaches or cyberattacks;
- Incident Response: Investigating and reviewing security incidents to determine their root causes and implementing corrective measures to prevent recurrence;
- Third-Party Assessment: Evaluating the security measures of third-party vendors and partners to mitigate external risks to the organization; and
- Security Audits: Conducting and coordinating regular internal and external security audits to assess the effectiveness of security measures and identify areas for improvement.

Training

Fostering a culture of security and privacy awareness within SEON is an integral part of safeguarding customer data. Given that SEON's service is fully data-driven, it is crucial that SEON employees have an in-depth knowledge of the privacy & security requirements, regardless of their position.

That's why SEON has established a Security & Privacy training program mandatory for all employees to complete annually, designed to heighten collective staff awareness regarding data protection and security and effectively address privacy compliance risks. Furthermore, SEON requires specialized onboarding programs for employees in critical roles, such as those in the Compliance Team and Security Team.

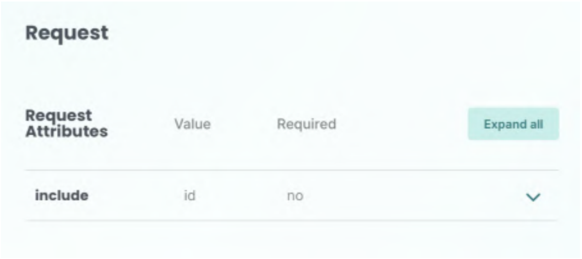
3.4 SEON's data architecture

Categories of personal data processed by SEON

The categories of personal data to be processed by SEON on behalf of our customers are determined by our customers as data controllers. Thus, this lies in their sole responsibility. All possible data points and categories of personal data are described on the SEON Documentation page.

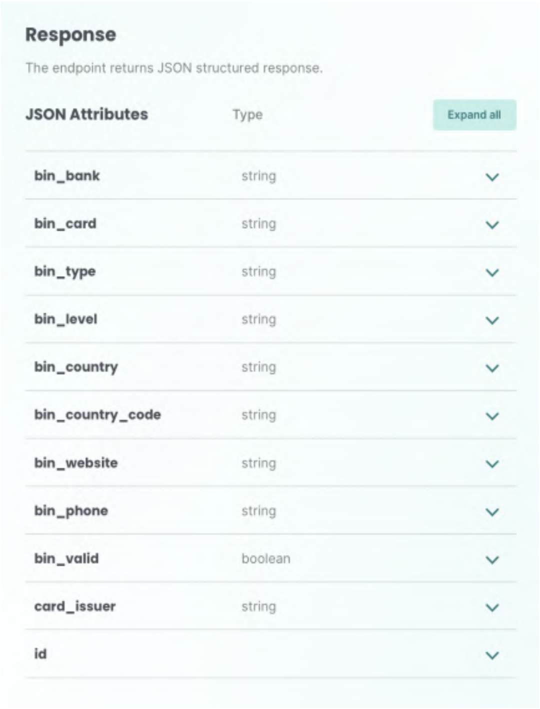
For each API type, you may find information on what categories of personal data are requested by our customer (Request) and what categories of personal data are returned to our customer by SEON (Response).

An example: Request and Response Data for the BIN API:



Request

Request Attributes	Value	Required
include	id	no



Response

The endpoint returns JSON structured response.

JSON Attributes	Type
bin_bank	string
bin_card	string
bin_type	string
bin_level	string
bin_country	string
bin_country_code	string
bin_website	string
bin_phone	string
bin_valid	boolean
card_issuer	string
id	

Data Localization, Data Residency

Customer data processed by SEON on behalf of our customers is being processed in a cloud environment provided by Amazon Web Services (AWS) with servers on EC2 instances and with relational database systems. The location of data processing is in Ireland, EU [EU-West-1. (EU country)] by default. However our customers may also choose Northern Virginia, US (AWS US-East-1) as data region as well.

Important information for financial institutions: SEON has entered into an EBA Financial Services Addendum with AWS, thus SEON is fully compliant with the guidelines set forth by the European Banking Authority (EBA). This assures financial institutions that they can utilize SEON services in strict accordance with the regulatory framework, meeting all necessary legal requirements.

In the relationship between AWS and SEON, the principle of shared responsibility applies, which means AWS manages the security and compliance of the cloud computing infrastructure, while SEON manages the security and compliance of the software and data residing in the cloud computing infrastructure.

By default, SEON offers its customers a multi-tenant solution, thus, infrastructure is shared between customer instances. To ensure data isolation and security, each customer's data and configurations are logically separated within the AWS environment with separate database tables for each customer. However, upon request and negotiation, our customers may subscribe to SEON's Premium Tier service, which entails providing an entirely distinct, standalone AWS account featuring a single tenancy.

Data life cycle

1. **Data Collection:** Data is being obtained by SEON

   a) Directly from the individuals interacting with us directly (e.g. creating a SEON account, using the look up tool on our homepage, signing up to our newsletter, registering to a webinar or applying to an open position at SEON etc.);

   b) Automatically from our customers with seamless integration of our services to the customer's digital flows (APIs) as described on the SEON documentation page.

2. **Data Ingestion:** Once the data is collected, it goes through the ingestion process, transforming it into a format suitable for processing. This may involve data cleaning, validation, and transformation to ensure accuracy and consistency.

3. **Data Storage:** The processed data is then stored in databases depending on the exact type of personal data. Data is stored in the AWS cloud infrastructure (see above). This stage ensures that the data is available for further processing and analysis when required. However, the maximum retention time (storage time) will never exceed the period set out in the Data Privacy Addendum or our Privacy Policy.

4. **Data Usage and Presentation:** The usage always depends on the specific data type. Regarding customer data, the analyzed data is presented meaningfully to end-users through reports, dashboards, visualizations, or other tools on our Admin Panel.

5. **Data Retention:** Our data retention policy determines the duration for which data should be retained in accordance with legal obligations or business requirements. By default, SEON stores customer data for 1 year unless our customer instructs us otherwise. During the retention period, the data remains accessible for the purpose of analysis or audit. Customers can also delete their data through the erase API endpoint or from the Admin Panel UI.

6. **Data Deletion:** When data reaches the end of its useful life or is no longer needed, it shall undergo secure deletion from all storage locations to uphold data privacy and adhere to data protection regulations.

7. **Data Destruction:** Sensitive data or data subject to stringent regulations necessitate using secure data destruction methods, including data shredding or overwriting, to guarantee that the data remains irretrievable.

Encryption in Transit and at Rest

Data is being encrypted both at rest and in transit. SEON applies AES-256 encryption of the data at rest and HTTPS connection and at least TLS 1.2 for the encryption of the data in transit.

3.5 Vendor Management and Sub-Processors

SEON utilizes vendors to provide certain services. Vendors include but are not limited to cloud providers and software providers. In some cases, SEON utilizes one-time vendors and some vendor relationships are ongoing. SEON undertakes appropriate actions to carefully choose and retain exclusively vendors who will adhere to and execute security measures in alignment with our internal policies and who have implemented appropriate safeguards regarding this.

This requirement holds even greater significance concerning SEON's sub-processors, given their access to customer data. To allow sub-processors to handle customer data trusted to SEON, each sub-processor must go under stringent annual due diligence, including legal, security, and privacy assessments. After due diligence, SEON concludes written contracts with the sub-processors at all times incorporating data protection provisions at least as protective as the privacy and security measures SEON has put into place.

Please find SEON’s up-to-date list of sub-processors in the Data Processing Agreement available on our website.

SEON ensures that no data transfers are carried out outside the EEA and has secured the same agreement with its sub-processors. Should data transfers outside the EEA be nonetheless necessary due to our customer’s location, appropriate safeguards shall be implemented for such transfers provided by Standard Contractual Clauses.

3.6 International Data Transfer (if applicable)

SEON will not transfer personal data outside the chosen data residency region and has secured the same agreement with its sub-processors. Should data transfers outside the EEA be nonetheless necessary due to our customer’s location, appropriate safeguards shall be implemented for such transfers provided by Standard Contractual Clauses.

If transferring data outside the EEA or the United Kingdom should be nevertheless necessary due to the customer’s location, SEON applies a range of protection mechanisms. These include written agreements with our customers and affiliates, Standard Contractual Clauses, and, where applicable, the European Commission’s adequacy decisions concerning specific countries.

3.7 The EU - US Data Privacy Framework

Concerning data transfer to the U.S., our U.S. affiliate, SEON Technologies US Inc., is in alignment with the EU-U.S. Data Privacy Framework, including the UK Extension to the EU-U.S. Data Privacy Framework established by the U.S. Department of Commerce for managing personal data transferred from the European Union, the European Union, the European Economic Area and United Kingdom to the United States. SEON has obtained a certification from the U.S. Department of Commerce, affirming its commitment to the Data Privacy Framework for such data. For further insights into the Data Privacy Framework and to access SEON's certification, please visit www.dataprivacyframework.gov.

3.8 Security Measures

SEON has established an efficient framework for managing information security and internal controls applying a number of technical security measures in order to avoid and minimize information security risks and to fortify our defenses against potential security incidents.

In the following paragraphs we would like to highlight the cornerstones of our security framework which help us protect our infrastructure and ultimately our customers:

Policies

Policies and procedures, such as Cyber Security Policy, Change Management Policy, Access Management Policy, Patch and Hardening Policy, Acceptable Use Policy, Data Protection Policy, Incident Management Policy, are defined regulating the security processes to create a unified understanding and accountability.

Awareness

To raise the general cyber security awareness of all SEON employees, our mandatory cyber security training covers the most important security topics. This training is to be completed at onboarding and to be repeated annually thereafter. Additionally regular awareness communications and security related announcements are made to keep security in the spotlight.

Access control

The best approach to prevent data leak is to narrow down the circle of people who have access to sensitive data. In order to do this, a strict access control workflow is implemented at SEON. Access rights are requested and approved in a centralized manner. There is a segregation of duty between the approver and the administrator setting the actual access right in the system which implements 4 eye principle in the process. Access rights are reviewed quarterly to discover any discrepancies.

All of our critical systems require multi-factor authentication and we utilize the additional security provided by SSO and a central identity provider wherever it's possible.

Vulnerability management

To keep our infrastructure secure we perform continuous vulnerability scans on all of our servers, managed cloud resources and container images. There is a regular patching process in place with an emergency fast track if a particular vulnerability requires instant remediation. Our security team stays current with the evolving threat landscape by regularly analyzing various security news outlets, industry blogs, information found on social media platforms, vendor announcements, CVEs, and government information sources.

Log management

Logs of security events are collected and stored in a centralized location with limited access to protect their integrity. They are analyzed and alerts are raised to the security team in case of suspicious events.

Secure development

The largest part of SEON's attack surface is its API and web UI. To keep both as secure as possible we implemented several measures in the development process. First of all our developers' awareness is raised to the typical software security issues and a comprehensive development security checklist is published on our internal knowledge base to serve as a guideline.

Static application security testing tool (SAST) is implemented in our CI pipeline to catch potential vulnerabilities before they are released.

We scan our repositories for committed credentials, and use secret stores to protect credentials and other sensitive parameters used by the application. Sensitive parameters are injected in the environment during deployment.

If a particular software component has security relevance our security team is involved from the beginning of the planning and design process and manual security tests are performed during the development.

To have an independent assurance about the security of our product, penetration tests are performed by external professionals at least annually, and findings are remediated with high priority.

Change control

Having a closed change control process is also a key element of security. We use GitHub as our version control system of choice. Branch protection rules are defined to protect the integrity of the source code and implement a 4 eye principle in the change process. No code without an independent review can be merged into the main branches from where the production environments are released. As we use infrastructure as a code for managing our workloads, this process also applies to infrastructure changes. Unit, regression and integration tests are performed in separated test environments on generated or anonymized test data sets to catch bugs before go live. We do blue-green and canary deployments to minimize the downtime and to give ourselves an easy and fast way to roll back if something goes south.

Data center security

SEON's infrastructure is designed as a fully cloud-native system, leveraging the expertise of Amazon Web Services in managing the underlying physical infrastructure that supports our virtualized workloads. Through the frequent evaluation of AWS's SOC 2 report and our trust in their specialized capabilities, we are confident in their ability to provide secure and reliable infrastructure support for our platform.

Encryption

We use industry standard encryption algorithms with key lengths which are based on the current NIST recommendations and best practices. Data in transit over insecure networks is encrypted with TLS 1.2 or 1.3, data at rest is encrypted with AES256. Passwords in our database tables are hashed using bcrypt. Certificates are using either RSA algorithm with a minimum key length of 2048 bit or ECC keypairs. Encryption keys and certificates are stored in secure keystores.

Network security

Securing a network is hard. We use different tools to raise the bar for our attackers and minimize breaches. We implemented subnet segmentation where only the components, mainly load balancers in the public subnets are reachable from the internet. Resources in the private subnets are micro-segmented using security groups which are identical to stateful firewalls. To protect our API endpoints and web UIs from layer 7 attacks we use WAF. IDS is used to inspect security and network logs and traffic and generate alerts in case of suspicious events, and there is an active DDoS protection in place.

Anti-malware

All of our workstations and servers directly reachable from the internet or processing file uploads from external users are protected by centrally managed anti-malware software. Both heuristic and pattern matching virus detection are performed, the virus definition databases are updated multiple times a day on the clients.

Backups

We prepare full backups of our databases daily and also perform WAL log archiving. In the case of a data loss, our team is equipped with the necessary tools and processes to promptly initiate the recovery process to minimize disruption and restore services as quickly as possible.

High-availability

To provide a robust and resilient service and to meet our SLA, we planned and built our infrastructure with high-availability and redundancy in mind. Our services are running in load balanced clusters which are stretched across multiple availability zones. This provides us geo-redundant infrastructure with active-active clusters with seamless switch over in case of an unhealthy node.

3.9 Information Security Incident and Personal Data Breach Management

In the event of data breaches, our dedicated Security Team will promptly and effectively address such situations in line with our applicable event management procedures and plans. We will adhere to our legal obligations by detecting the incidents, gathering information about it, planning and executing our response measure, promptly reporting these incidents to regulatory authorities and also ensuring timely notification to affected customers, users, or other relevant parties. Following the resolution of these incidents, a comprehensive review and documentation will take place, leading to the implementation of pertinent measures to mitigate the risk of similar events recurring.

3.10 Data Subject Rights

Our obligations as data controllers

When SEON acts as a data controller concerning the personal data of the individuals using our services, visitors to our website, social media sites, webinar participants and any other persons who interact with us directly, we take responsibility for the processing of personal data in its entirety and for complying with the applicable data protection laws.

If the data subjects wish to exercise any of their rights under the applicable data protection laws (e.g. right to access, right to erasure etc.) they may contact us at compliance@seon.io or at dpo@seon.io. SEON’s compliance team is responsible for the management and operation of this channel to handle the data subject requests and ensure that the responses align with the applicable privacy laws.

Our obligations as data processors

When SEON acts as a data processor concerning customer data, the data subjects may assert their rights by contacting our customers as data controllers. However, if the data subjects contact us directly, we will promptly inform the respective customer (data controller) about such requests and will, in accordance with the Data Processing Agreement, comply with their instructions.

4. Certifications

SEON has successfully acquired multiple internationally acclaimed certifications in security and privacy compliance, affirming our enduring dedication to maintaining robust security standards and preserving individuals' privacy. We may share these certifications with our stakeholders whenever possible.

ISO 27001		SOC 2 Type 2
ISO 27001 enjoys broad recognition within the information security management sector as a globally respected accreditation. Like other ISO standards, ISO 27001 is only optional in fraud tech. At SEON, however, we believe all our clients, partners, and investors should trust that we are dedicated to meeting the best security standards and have successfully fulfilled the security criteria mandated by this certification.		The SOC (System and Organization Controls) report is an independent evaluation of an organization's internal controls conducted by a third party in accordance with the assurance standards set by the American Institute of Certified Public Accountants (AICPA). This assessment provides assurance regarding the organization's control environment. SEON's SOC 2 (Type 2) report affirms that SEON adheres to the essential principles of security, availability, confidentiality, and privacy concerning its system and internal control, aligning with the mandated standards outlined in SOC regulations.

5. Conclusion

Protecting personal data is our highest priority, ensuring our effective role as our customers' efficient fraud prevention tool. We've invested significant effort into upholding a robust privacy compliance and security framework at SEON, implementing technical and organizational safeguards to protect personal data processed by us.

We trust this document has granted valuable insight into our approach to privacy at SEON. As we advance, our commitment is to enhance further our privacy and security compliance program with a dedication to transparency.

Should you have any additional queries regarding our privacy and/or security approach or how we handle the personal data entrusted to us, please do not hesitate to contact our Compliance Team at compliance@seon.io or our Data Protection Officer at dpo@seon.io.

If you want to learn more about the SEON service, contact our Sales Team at info@seon.io.

Additional information

- SEON Terms and Conditions https://seon.io/resources/legal-and-security/legal/#h-service-level-terms
- Data Processing Agreement (including list of sub-processors and Standard Contractual Clauses)
  https://seon.io/resources/legal-and-security/legal/#h-data-processing-agreement
- SEON Privacy Notice
  https://seon.io/resources/legal-and-security/privacy/#privacy-policy
- SEON Code of Business Ethics
  https://seon.io/resources/legal-and-security/code-of-business-ethics/#code-of-business-ethics