Security and Compliance Whitepaper

TABLE OF CONTENT

AppXite recognizes data as one of the most valuable assets, protection of which plays a vital role in sustaining business, driving success, securing customer trust and complying to regulatory requirements. Protecting data is therefore also a cornerstone of our product delivery and by using AppXite platform to power your business you can remain confident that your data is secured.

Nicolas Albana, CEO

1. Introduction

There is no doubt that the rapid adoption of cloud technologies leads to significant changes in data processing environment. The nature of the cloud business requires providers to aggregate and process massive amount of data, including personal data. That is why, besides all the benefits that comes with using cloud-based products, it is paramount to select a partner which believes that security, privacy and compliance must form an integral part of its product.

To maintain the trust of our customers and partners AppXite is committed to make security, privacy and compliance controls the integral part of our product design.

Besides powering your subscription-based business, automating processes, reducing costs, and increasing productivity, AppXite platform is designed to ensure complete data security, privacy and integrity and provide you with the effective data management tools to help you to meet the regulatory compliance.

AppXite has implemented a set of tools to ensure that customer data is processed in a secure, confidential and transparent manner. AppXite ensures that its products are build according to the *"Privacy by Design"* and "*Privacy by Default*" principles and enable customers to manage their data and exercise data subject's rights according to the General Data Protection Regulation ("GDPR").

The objective of this whitepaper is to provide our customers and partners the comprehensive overview of security and compliance measures taken by AppXite to protect data.

2. AppXite Security Team

AppXite has a dedicated security team that is responsible for administering internal policies and procedures, monitoring systems related to security, respond to any security related inquiries, handle security incidents and detect bugs. The scope of Security Team responsibilities includes:

- Participating in the product design to ensure that our products are developed in accordance to the "*Privacy by Design*" and "*Privacy by Default*" principles.
- Administering internal audits to review compliance with privacy laws, *Best Industry Practice* and widely recognized information security standards.
- Handling vulnerability management to pro-actively identify, log, communicate and prioritize security vulnerabilities. For that purpose, AppXite is using a combination of automated vulnerability monitoring tools, quality assurance, external penetration tests, manual monitoring routines and external/internal audits.
- Reviewing logs to identify unusual behaviour within AppXite systems and products.
- Developing and managing business continuity and disaster recovery plan.
- Handling incident management to detect, contain and eradicate security events.

3. Security Culture and Awareness

AppXite has built a strong security culture for the entire organization. All AppXite employees undergo security training as part of their onboarding process and throughout their employment.

All new employees are bound by confidentiality obligations and agree to conform to AppXite's internal policies which include Information Security Policy, GDPR processes, processes pertaining to access management and secure development practices. AppXite carries out bi-annual security training for all employees to ensure that employees acknowledge the importance of information security, refresh their knowledge and at all times remain aware of the new information security threats. Our CISO attends security related presentations and events to maintain the knowledge and expertise in the security area.

4. Information Security Strategy

AppXite has implemented the information security strategy which contains clear goals and objectives for strengthening security of AppXite products. The strategic goals and objectives include:

- Keeping policies and procedures up to date and fit for purpose. This includes monitoring the regulatory framework to ensure that our control arrangements are in conformity with the applicable law.
- Proactive detection of security weaknesses at all stages of product delivery.
- Implementing additional security controls within AppXite Platform.
- Scheduled information security trainings to all employees to ensure the high level of security and privacy awareness among employees.
- Ensuring respect for privacy and effective data management within the entire customer data lifecycle.

5. AppXite Security Team

Access to customer data is strictly restricted and granted solely based on the principles of "need to know" and "least privilege". Every employee that access customer data is bound by confidentiality obligations and is subjected to extra training to minimize the human error. In addition, AppXite provides its customers fine-grained security controls to manage permissions to different customer resources with respect to internal organization. Learn more about role-based permissions here: User Permissions and Roles.
Among different log in options, AppXite supports log in with Azure Active Directory account: How to log in with work email. By doing so, customers can log in to the AppXite platform by using the same authentication credentials as those used to log in to the local Azure AD.

6. Supplier Management

AppXite procurement processes involve third-party supplier verification in terms of information security. Prior to signing a contract with a third-party supplier, AppXite requires such supplier to submit a checklist which includes the set of security/privacy requirements that are equivalent or better than those implemented by AppXite. Once an assessment is made, AppXite proceeds in onboarding a supplier.

All suppliers that process data on behalf of AppXite are bound by strict confidentiality obligations. If such data includes personal data, AppXite and supplier enter into *Data Processing Agreement* (including EU Model Contract Clauses if applicable) according to the Article 28 (3) of the General Data Protection Regulation.

7. Data Encryption

All customer data is classified as strictly confidential and subject to encryption in transit.
Considering that data may be intercepted in transit or monitored as plaintext data transmitted across unencrypted network, any transfer of data through a network is encrypted according to the industry-accepted encryption mechanism TLS 1.2. Monitoring tools are implemented to detect any malicious attempt to access customer data.

8. Activity History

AppXite Platform provides a customer with a comprehensive overview of actions and events associated with its platform. This tool is designed to provide partners with an audit trail to detect any malicious acts or human error that results in changes to customer profile, orders, products and billing data. AppXite will take its commercially reasonable effort to extend the list of logged activities that are available for partners. Nevertheless, partner can request AppXite to provide logs related to any activity pertaining to partner's platform account.

9. Two-Factor Authentication & Password Strength Policy

AppXite Platform supports various identity providers, that allow customer to configure password policies, such as password length, password complexity (e.g. combination of numbers, letters and special characters), session timeouts, password expiration and prevention to use a recently used password. Password policy configuration is dependent on customer's identity provider configuration.
User accounts are locked after several unsuccessful attempts. In addition, partners can enable multi-factor authentication that requires user to have both login credentials and code sent via SMS to authenticate.

Therefore, confidentiality is further ensured by means of identity and access management, using strong authentication mechanisms. It is also suggested that data processors' employees and contractors must be bound by confidentiality obligations.

10. Independent Third-party Certifications

In order to maintain the holistic security and compliance frameworks, demonstrate our commitment to the *Best Industry Practice* and strengthen regulatory compliance, AppXite undergoes independent third-party audits under the following international standards: ISO 27001, ISO 27017, ISO 27018, ISO 20000-1 and ISO 9001. The scope of certification includes all AppXite's processes, systems and products.

ISO 27001:2013 – Information Security Standard which establishes a framework of security controls to safeguard internal and external data. Our ISO 27001 certificate is available Here.

ISO 27017:2015 – Code of practice for information security controls based on ISO/IEC 27002 for cloud services, which provides additional cloud-specific implementation guidance based on ISO/IEC 27002 and provides additional controls to address cloud-specific information security threats and risks considerations.

ISO 27018:2019 – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors which establishes control objectives, controls, and guidelines for implementing measures for the protection of PII in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment and taking into consideration the regulatory requirements for the protection of PII which can be applied within the context of the information security risk environment(s) of a provider of public cloud services. Our ISO 27018:2019 certificate is available Here.

ISO 20000-1:2018 - Information Technology Service Management Standard which requires AppXite to ensure that service design, transition, and delivery fulfill the service requirements. Our ISO 20000-1 certificate is available Here.

ISO 9001:2015 - Quality Management Standard which requires AppXite to ensure that our products and services consistently meet the Best Industry Practice and that service quality is continuously improved. Our ISO 9001 certificate is available Here.