Vatix Security – Commitment to Customer Trust

Posted as of: 14 March 2024
Effective as of: 14 March 2024

Contents

1 Introduction

In the digital era, organisations of every size and from various sectors are leveraging the power of cloud services. The access to cutting-edge technological solutions and superior infrastructure management they provide facilitates rapid innovation and scalability, essential for meeting market demands. Furthermore, cloud service providers can offer high security standards that many organisations may find challenging to achieve with their in-house IT teams or systems. Amid the shift towards a fully digital, work-from-anywhere environment in a progressively intricate landscape of cyber threats, organisations can significantly benefit from the secure infrastructures and stringent security practices offered by trusted cloud service providers.

At Vatix, we fully understand the crucial importance of adopting industry-leading security practices and technology to safeguard our customers' data. Our security measures are seamlessly integrated into all our technology, programmes, and processes. We offer an extensive range of trusted SaaS solutions for managing Environmental, Health, Safety and Quality (EHSQ) and operations, reinforcing the safety and well-being of employees in various environments. Our clients rely on us to maintain the highest standards of data integrity, confidentiality, and availability.

For years, we've partnered with clients in highly regulated industries such as government bodies, financial services, healthcare, and utilities. Each of these clients entrusts Vatix with their data, testament to the trustworthiness of our services.

As a provider of technology solutions and services, our business's foundation is the continued provision of secure, reliable, and compliant services that safeguard customer data and foster customer trust. This document offers a comprehensive overview of our security strategy, programmes, and controls. It highlights how our organisational values steer our commitment to achieving excellence in securing our customers' data and privacy, including adherence to the General Data Protection Regulation (GDPR) and our unyielding commitment to data privacy.

We take our privacy obligations – both legal and contractual – extremely seriously. We are active in ensuring compliance with data protection laws and maintain our ISO/IEC 27001:2017 accreditation, representing our commitment to the highest standards in data security.

This document is intended to serve as an initial point of discussion for more extensive and in-depth security discussions. It should reassure you of our active and steadfast dedication to our privacy obligations and data protection.

2 Company Registration and Location

Vatix Limited is a company registered in England and Wales. Our registered office is situated at 30 Great Guildford Street, London, SE1 0HS, United Kingdom. Our company registration number, as listed on the register at Companies House, is 11698437.

3 Data Protection Compliance and ICO Registration

As a company registered in England and Wales, we comply with the UK data protection regime which includes the UK GDPR and the Data Protection Act 2018 and our services will be provided in accordance with these laws.

We are registered with the UK Information Commissioner (ICO) under number **ZA521690**.

The UK regime has been deemed adequate by the European Commission and, as such, if your organisation is in the European Economic Area (EEA), you should be reassured.

If your organisation is based outside of the UK or EEA, we are happy to discuss what, if any, additional protections you may need to comply with the data protection legislation of your territory.

4 Adherence to Quality and Security Standards

Vatix is accredited to BS EN ISO/IEC 27001:2017, certificate number 225267, and this certification is accredited by the UKAS (United Kingdom Accreditation Service) body. ISO/IEC 27001:2017 is an international standard that outlines best practices and comprehensive security controls following the ISO 27002 best practice guidance. This accreditation demonstrates Vatix's commitment to an ongoing and systematic approach to managing and protecting company and customer information.

Furthermore, Vatix's Lone Worker application, associated services, and devices are compliant with the British Standard BS8484: 2022, also known as the 'Code of Practice for the provision of lone worker device services'. Further details regarding this standard can be viewed at https://www.bsigroup.com.

Adherence to these standards underscores Vatix's commitment to delivering quality, reliability, and integrity in its service provisions, providing you, our clients, with the utmost assurance in our capabilities.

5 Our Organisational Structure for Ensuring Data Protection Compliance

Ensuring the protection of our clients' data lies at the core of Vatix's operations. We maintain a robust culture of compliance, intricately woven into our software, systems, and procedures.

Vatix has diligently established a UK GDPR compliance framework, underpinned by internal policies and procedures dedicated to compliance and information security. These policies have received Board approval and undergo regular reviews to maintain their relevance and effectiveness.

As an integral part of our commitment to security, Vatix is accredited to BS EN ISO/IEC 27001:2017, affirming our dedication to the rigorous standards of this international information security standard. Our certification extends to multiple areas of our Information Security Management System (ISMS) which includes:

a) Information security policies
b) Organisation of information security
c) Human resource security
d) Asset management
e) Access control
f) Cryptography
g) Physical and environmental security
h) Operations security
i) Communications security
j) System acquisition, development, and maintenance
k) Supplier relationships
l) Information security incident management
m) Information security aspects of business continuity management
n) Compliance with both internal requirements, such as policies, and external requirements, such as laws
o) Our personnel undergo regular training to ensure they understand the importance of data protection and are adept at applying its principles in their roles. As law, commercial practices, or our offerings evolve, training is updated to keep pace with these changes.

A designated privacy officer guides Vatix on matters of compliance, and we have access to specialist external legal support when needed. We monitor our compliance through various activities, including internal auditing and incident analysis. This structure ensures the persistent integrity of our clients' data and maintains our commitment to the highest standards of data protection.

6 Understanding Vatix's Role as a Data Processor

As your service provider, Vatix assumes the role of a data processor for all personal data stored within your account in our application. You, our client, remain the data controller. All activities involving the processing of your personal data are conducted strictly according to your documented instructions, as established in the contract between us.

For the purposes of system enhancement, Vatix may anonymise and aggregate data within our systems. These actions facilitate a more profound understanding of system usage, enabling us to develop our offerings to align with our customers' needs, ensure optimal data security, and address potential issues in a timely manner.

Importantly, Vatix adheres to stringent data protection and privacy standards. We refrain from using any of the personal data you entrust to us for direct marketing purposes, unless we have received explicit consent from either you, the data controller, or the individual data subject.

7 Vatix Risk Assessments to Safeguard Personal Data

In accordance with the privacy by design and default requirements of the UK GDPR and our ISO/IEC 27001:2017 accreditation, Vatix has developed our software and services to mitigate potential risks to personal data and data subjects. To this end, we have embedded an array of security measures designed to protect data.

We conduct regular risk profile reassessments as our applications evolve to ensure our continued alignment with the requirements of ISO/IEC 27001:2017 and our obligations under data protection law. Any modifications to the risk profile of our products mandate approval from our Board, maintaining a level of executive oversight.

8 Is there a requirement for a Privacy Impact assessment?

Our applications and services seek to obtain very limited personal data but there are a number of data fields that are free text and could, potentially, be used by your users to record special category data or other sensitive information. You will need to ensure that you have carried out a data protection impact assessment where necessary to address this and will need to ensure your users only use the service to record details for which you are satisfied meet your risk profile.

9 Ensuring UK GDPR Compliance Across Vatix Systems

Vatix has performed a comprehensive Privacy Impact Assessment on our software, systems, and services, and has implemented necessary adjustments to ensure compliance with, and in some cases exceed, UK GDPR requirements.

Our system architecture, developed in alignment with ISO/IEC 27001:2017 standards, prioritises data protection and security. Databases containing your personal data are accessible solely by a select, vetted segment of our development team. Live data is not utilised for testing, nor is it stored on local machines, ensuring the highest level of data protection.

10 Data Retention Policy and Practices at Vatix

Vatix implements a comprehensive data retention policy in line with the necessary legislation, reflecting our commitment to robust data protection practices. Generally, Customer Personal Data associated with a specific Vatix service is deleted within 60 days following the termination of the respective service agreement. However, the exact terms and conditions governing data retention can vary and are elaborated in full in the Vatix Master Services Agreement. For a complete understanding of our data management practices, we strongly recommend that all customers review these terms, as they have been designed in compliance with our ISO/IEC 27001:2017 accreditation and applicable data protection laws.

11 Location and Process of Personal Data Handling at Vatix

Vatix is committed to ensuring the secure and compliant processing of your personal data. Except for specific provisions pertaining to overseas customers for whom we offer dedicated in-country services, all live customer personal data is stored within the UK. To host our data and applications, we utilise Amazon Web Services, specifically within the London region, in compliance with our ISO/IEC 27001:2017 accreditation.

We work with select sub-processors who are tasked with performing certain activities integral to our service delivery. These sub-processors are carefully chosen and managed to ensure they align with our stringent data security standards. For your convenience, we maintain a comprehensive list of these sub-processors, which can be accessed at: https://vatix.com/legal/sub-processors/

Security Measures

12 Security Education and Awareness

At Vatix, the security of our customers' data is a paramount concern. We firmly believe that our employees constitute a crucial line of defence in this respect. To enhance the security consciousness of our workforce, we have instituted a comprehensive program that includes new employee onboarding, annual security training, role-based awareness education, and phishing simulations.

13 Data Center Security

Our commitment to data security extends to the selection and management of our data centres. We rely on trusted third-party infrastructure service providers such as Amazon Web Services, which align with our ISO/IEC 27001:2017 accreditation. These centres, located strategically across various geographic locations, ensure redundancy and robust physical security. Features include controlled access, CCTV monitoring, and biometric controls, guaranteeing the security of your data at all times.

14 Network Security

Vatix adheres to industry best practices in our network and host security measures. Customers access our services via the public internet, using Transport Layer Security (TLS) for secure connectivity. Our data traffic is routed through firewalls and routers to bolster our security perimeter.

15 Distributed Denial-of-Service Protection

We adopt a multilayered approach to Distributed Denial of Service (DDoS) protection. By utilising multiple internet service providers and consistently monitoring network traffic, we ensure any anomalies are swiftly detected. Furthermore, our deployment of a DDoS mitigation service reduces the risk of these potential attacks significantly.

16 Penetration Testing

Vatix is devoted to maintaining a high level of security across our services. To this end, we conduct regular internal vulnerability scans and penetration tests. Moreover, we engage the services of an independent, CREST-certified cyber security consultancy to perform an external penetration test at least once each year. These thorough examinations of our security measures help ensure that we are continually vigilant and proactive in the protection of our customer's data.

17 Infrastructure User Access, Identification, and Authentication

Access to our production environments is tightly controlled and regulated. Only employees with a legitimate requirement are granted access. Such privileged employees, like our site reliability engineers, are required to use multiple layers of two-factor authentication. This access control strategy reflects our adherence to the Principle of Least Privilege and Segregation of Duties.

In conclusion, Vatix’s commitment to stringent security measures and adherence to our ISO/IEC 27001:2017 accreditation ensures robust protection and integrity of customer data. We are unwavering in our pledge to maintain the highest level of data security and to sustain the trust you place in our services.

18 Data Backup Measures

To further strengthen our data protection measures, Vatix operates a robust data backup system. All customer data is replicated to ensure there is always a duplicate copy available. Moreover, we regularly conduct snapshot backups in accordance with industry best practices. This method ensures that an up-to-date copy of data is always available, adding an extra layer of security and resilience in the unlikely event of data loss. Our backup strategies form part of our overall commitment to data protection and compliance with the BS EN ISO/IEC 27001:2017 standards.

19 Customer Authentication Options and Responsibilities

At Vatix, we offer several methods for secure user login, each designed to strike a balance between user convenience and robust data protection:

- **Email and Password:** Our standard login procedure involves users creating a unique password, which is used in combination with their registered email address to access the system.

- **Two Factor Authentication (2FA):** For enhanced security, we also offer Two Factor Authentication, which necessitates users to input a verification code sent via SMS during the login process.

- **Single Sign-On (SSO):** For a seamless login experience, Vatix supports Microsoft's Azure Active Directory SSO user authentication solution. This enables users to access multiple applications using a single set of credentials.

As the account holder, it is your responsibility to ensure the security of your login credentials, and you will be accountable for all activities occurring under your account. It's important to note that the Two Factor Authentication and Single Sign-On features are subject to additional charges. For more information on these services, please consult your Vatix sales or success representative.

Personnel and use of Sub-contractors

20 Staff Data Handling and Confidentiality

In line with our robust data protection practices, every member of the Vatix team, including our contractors, is obliged to sign an agreement that includes confidentiality clauses relevant to the data we process on your behalf. These confidentiality agreements, complemented by contractual obligations to comply with our rigorous data security measures, ensure a consistent and dependable standard of data handling across our organisation.

21 Subcontractor Engagement and Data Security

While we take pride in providing most of our services in-house, certain elements, particularly those ensuring the security of hosted data, are entrusted to select third parties. Our choice of subcontractors reflects our commitment to delivering top-tier services and robust data protection.

A detailed list of these subcontractors, the services they provide, and the location of data processing can be accessed at https://vatix.com/legal/sub-processors/.

We ensure that every subcontractor we engage with is thoroughly vetted and authorised by a designated Vatix representative during our supplier onboarding process. Furthermore, we maintain formal contracts with each subcontractor that incorporate stringent data protection provisions to safeguard your personal data.

Contracting

22 Incorporation of Data Protection Provisions in Our Contract

Our contractual relationship with you encompasses multiple documents such as the Master Service Agreement (accessible at https://vatix.com/legal/agreements/master-service-agreement/) and a Data Processing Addendum, often referred to as the 'DPA', which can be viewed at https://vatix.com/legal/agreements/data-processing-agreement/. The DPA encapsulates all the provisions that the UK GDPR necessitates, ensuring you, as the data controller, include these in your contract with us, the data processor. This robust contractual framework ensures we fulfil our mutual legal obligations.

23 Assisting in Compliance with Data Subject Rights

As our client, you have absolute control over your user data and, thus, should be fully equipped to manage all data subject rights through the use of our application. However, should you require additional support, our team stands ready to assist, although please note that additional charges may apply.

24 Audit of Vatix's Premises and Systems for Compliance

We underscore the importance of maintaining the confidentiality and integrity of all our customers' information. To this end, we typically do not allow customers to access our systems or premises directly. However, to assure our compliance, we undergo annual audits following the ISO/IEC 27001:2017 and BS8484:2022 standards, which verify our adherence to best practices in information security and service provision for lone workers.

Upon request, we are more than willing to provide our latest certificates from these audits for your peace of mind. It's important to note that in scenarios where a court or regulatory body necessitates us granting you access, we will abide, whilst mandating your compliance with our security and health and safety requirements.

Data Breaches

25 Procedure for Addressing Suspected Unauthorised Data Access

In instances where unauthorised access to your data is suspected, immediate notification to the relevant admin user is critical. Given their comprehensive control over user access rights, your admin user is responsible for promptly reviewing and, where necessary, disabling the access of any implicated users.

Vatix retains the capability to enforce user access restrictions as required. Should this course of action become necessary, please contact us at support@vatix.com.

26 Vatix's Protocols in Response to Potential Data Breaches

While Vatix upholds an exemplary record with no reportable data breaches to date, it is fundamental to maintain vigilance and preparedness for any potential security incidents.

Should a security incident or system-wide issue occur, a detailed Major Incident Report will be created. This report will encompass an analysis of the incident's nature, its impact on your business and data subjects, the resolution, and proposed preventive measures to avoid a repeat incident. We will also assess the requirement to report the breach to the Information Commissioner and/or affected individuals.

In the unlikely event that your personal data is impacted by a data breach, we commit to communicating this to you promptly and in line with our established support procedures.

Contact Information

For any general enquiries related to this document: Please email legal@vatix.com

For any data protection related enquiries: Please email dpo@vatix.com