

Posted as of: February 09, 2022  
Effective as of: February 09, 2022

As a provider of technology solutions and services, our business depends on the continued provision of secure, reliable and compliant services that protect customer data and promote customer trust. These FAQs should reassure you that we take our privacy obligations – both legal and contractual – very seriously and that we are active in ensuring data protection law GDPR compliance.

## About us

### 1 Where is Vatix based?

Vatix is a company registered in England and Wales and can be found on the register of companies at Companies House under number **11698437**.

### 2 What data protection regime will apply?

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 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.

### 3 Does VatiX adhere to any specific standards?

Our Lone Worker application and associated services and our devices comply with British Standard BS8484: 2016, also known as the '**Code of Practice for the provision of lone worker device services**'. You can find out details of this Standard at <https://www.bsigroup.com>

## Governance

### 4 How is VatiX structured to ensure data protection compliance?

The protection of our clients' data is at the heart of our business. We have a strong culture of compliance, which is embedded within our software, systems and processes.

We have worked hard to establish a UK GDPR compliance framework with internal policies and procedures for compliance and information security that are approved by our Board and kept under review. We designed and implemented an, ISO27001 compliant, Information Security Management System (ISMS) to ensure our systems and processes are following industry best practices when it comes

to information security.

Our personnel are trained to understand the importance of data protection and to apply its principles within their roles. Training is refreshed as the law, commercial practice or our offerings change.

We have designated a privacy officer to guide our business on compliance and have data protection specialist external lawyers that we can call on for additional support. Compliance is monitored through various activities, including internal auditing and analysis of incidents.

## **5 What is Vatix's role in respect of our data?**

You are the data controller of all personal data held in our application under your account and Vatrix is your data processor in respect of all the services provided to you. Our processing of your personal data is only on your documented instructions as set out in the contract between us.

We may anonymize and aggregate data within our systems so that we can ensure we understand how our systems are used, to enable us to make decisions about how to develop them to suit our customers' needs, to ensure adequate security for the data held and to deal with any concerns.

We do not use any of the personal data you entrust to us for direct marketing unless we have consent to do so from you or the individual whose personal data we use.

## **Our systems and services**

## **6 What risk assessments have been done to ensure personal data is protected?**

We are very mindful that the nature of our products, especially our Alarms product and service, may involve monitoring of individuals. Our software and services have been developed with full recognition of the privacy by design and default requirements of the UK GDPR in order to contain any risk to personal data and data subjects. We have incorporated a host of security measures to ensure data is protected.

As our applications evolve – we revisit the risk profile to ensure we continue to meet the BS8484: 2016 standard and our obligations under data protection law. Our Board is required to sign off on any changes to the risk profile of each of our products.

## **7 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.

## **8 Are the systems provided and used by Vatrix UK GDPR compliant?**

We carried out a Privacy Impact Assessment of our software, systems and services and have made changes to ensure we meet and, in some cases, exceed UK GDPR requirements.

Our system architecture was developed with data protection and data security in mind. The databases in which your personal data is stored are only accessible by a small division of our development team who are internally vetted. We do not use live data for testing and it is never stored on local machines.

### 9 Where will our personal data be processed by Vatix?

Apart from the overseas customers for which we provide a dedicated in country service, all live customer personal data is stored in the UK and we use Amazon Web Services (London region) to host our data and applications. Other sub-processors are instructed by Vatix to perform specific activities in order to deliver the services. A full list of sub-processors is available via <https://vatix.com/legal/sub-processors/>

### 10 What does Vatix do to protect login credentials?

We offer a number of log-in options:

- **Email and password** – this is our standard approach to login security. The user sets a password and uses the combination of their email address and password to log into the system
- **Two Factor Authentication (2FA)** – this requires users to enter a code sent to them by SMS when logging into the system
- **Single Sign-On (SSO)** – the Vatix services support Microsoft's Azure Active Directory SSO user authentication solution.

Ultimately, you are responsible for ensuring your users keep your account log-in credentials secure and for any activities or actions occurring under your account.

### 11 What does Vatix do to keep customer data secure?

We have a suite of security measures in place. These are kept under review and, wherever we consider it appropriate, they are enhanced. Full details are in our Security Measures document which we maintain to show our latest security improvements. If you would like to see a copy, please email us at [legal@vatix.com](mailto:legal@vatix.com). The following should give you an idea of how we protect your data:

Vatix encrypts, using industry-standard encryption tools, all sensitive data in transit and at rest. Sensitive information is encrypted by an SSL connection when in transit over public networks with SSL connections using TLS v1.2 or above.

Vatix Services are hosted in a secure data center managed by Amazon Web Services, with 24x7 security. Physical access to the network is strictly limited and monitored. Private networks are strictly segmented according to function. Restrictive firewalls protect communication entering the network and between private networks. All access to Vatix's network and services is strictly logged. Audit logs are reviewed on a regular basis. Internal and external penetration tests are performed on a regular basis by third parties. Two-factor authentication and strong password controls are required for administrative access.

### 12 What back-ups does Vatix take?

Vatix carries out backup continuously. Whilst our main datastore holds replicas of data at all times, we also run our other databases with duplicate data in ready to swap over should the need arise.

Multiple snapshots of the entire database are taken every day and we store them on a separate server

from the one that holds live data.

From these various back-ups, we can restore the entire database in the event of a major incident. We test our disaster recovery at least annually.

## Personnel and use of subcontractors

### **13 What does Vatrix do to ensure its staff are reliable when handing your personal data?**

All of our employees and contractors are required to sign a confidentiality agreement or an agreement with appropriate confidentiality undertakings that will cover the data that we will be processing for you. They are also contractually required to comply with our data security measures (or measures that are at least as stringent).

### **14 Does Vatrix rely on third parties to provide its services?**

Most of our services are provided in-house but we do use some third parties to provide certain aspects – most notably to ensure hosted data is secure.

Our latest list of subcontractors, the services they each provide for us and the location of the processing can be found at <https://vatrix.com/legal/sub-processors/>

Each of our subcontractors has been vetted and authorised by a designated approver within Vatrix as part of our supplier on-boarding process and we have written contracts with each of them incorporating appropriate data protection provisions to protect your personal data.

## Contracting

### **15 Does our contract with you include data protection provisions?**

Our contract is made up of a number of documents such as our Master Service Agreement, an Order Form and a Data Processing Addendum or 'DPA'. Our DPA sets out all of the provisions that the UK GDPR requires you, as a data controller, to include in your contract with us as your data processor so that we can all be satisfied that we are meeting our legal obligations.

### **16 Will Vatrix help us comply with data subject rights?**

You have full control over your user data and data from your users so you should be able to manage all data subject rights yourself just by using the application.

If you need any additional help – we are happy to support you but there may be a charge.

### **17 Will we be able to audit Vatrix's premises and systems for compliance?**

You will appreciate how important it is that our systems and premises ensure confidentiality for all of our customers and we do not normally allow customers to have access. We do, however, engage an external specialist to check our systems and provide a report on compliance each year and we are happy to make that available to you for your peace of mind.

Of course, if a court or regulatory body requires us to give you access, we will honour that requirement

but will require you to comply with our security and health and safety requirements in doing so.

## Data breaches

### **18 What should we do if we believe someone has gained unauthorised access to our data?**

Your admin user has full control over access controls for other users on your account. It is important that, if any users leave your organisation, their access should be reviewed and, if appropriate, disabled.

If you believe there has been unauthorised access to your account or any user data, you should notify your admin user immediately and they should make sure that passwords for the affected users are changed without delay.

Vatix can lock user access if necessary. You can contact our helpdesk if you need us to do so.

### **19 What procedures does Vatix have in place to deal with data breaches?**

We are proud of our record of having no reportable data breaches to date. However, we know the importance of being prepared for an incident.

All security incidents and platform wide issues will be recorded in a Major Incident Report which will cover: the nature of the incident, the impact on your business and data subjects the resolution and any preventative action planned to avoid recurrence. We will also make an assessment as to whether the breach must be reported to the Information Commissioner and/ or affected individuals.

In the event of a data breach affecting your personal data, we will report this to you without undue delay through our normal support process.