Blue10 B.V.
Oude Middenweg 17
2491 AC Den Haag | NL

T +31 (0) 88 258 31 00
compliance@blue10.com
www.blue10.com

KVK 27195343
BTW NL809410199B01
ING Bank NL06INGB0683496832

WHITEPAPER

Security & Privacy

Version 1.0
22 October 2022

1. Introduction

At Blue10, we believe in the power of automation. We develop software that help our clients eliminate manual and repetitive work, even within our own organization, we are continuously striving to automate repetitive work. We use cloud applications as much as possible in our customer services as well as in our own internal office applications. The Blue10 service is entirely based on cloud technology, working towards a fully automated CI/CD (Continuous Integration / Continuous Delivery) process. That is our infrastructure, and therefore having and providing a secure and reliable service is an essential principle for us which stands forefront in our attention every day. Security, availability and reliability are our raison d'être.

In this white paper, we give you - our current customer as well as a prospective one - insight into the key measures we have taken to ensure information security and privacy in our working practices, our processes, and our systems and infrastructure.

2. Table of contents

3. Employees

A secure environment, where information is handled with care, starts with our employees. During the onboarding of new colleagues, we pay attention to screening and emphasize the importance of information security and privacy. Every Blue10 employee signs a non-disclosure agreement and we require a certificate of conduct from employees who have access to client data. In team meetings, we regularly pay attention to security and privacy to keep the level of knowledge and awareness of our people updated. If necessary, our employees take part in specific training courses in order to adequately perform their work at Blue10.

4. Information Security Policy

Blue10 has its principles regarding information security recorded in its policies and actively monitors compliance with them. Part of these policies are procedures regarding change management, incident management, logical and physical security and continuity. The information security policy is periodically reviewed by management based on recent developments and threat parameters.

5. Cloud only

Blue10 offers a Cloud product to its clients and also internally only cloud applications are used. This is, also from a security perspective, a very deliberate choice. We do not have an on-site infrastructure or an in-house datacenter, but we use public cloud services from renowned parties, most notably Microsoft Azure. This applies to both the development of our service and the operational management. Blue10 uses the PaaS (Platform as a Service) services from Microsoft Azure as much as possible. Here, the security on infrastructure level is taken care of by MS Azure which strongly decreases the chance of configuration errors and other security risks. Blue10 is hosted on the Azure location Western Europe (Amsterdam). For more information regarding the security measurements from Microsoft Azure, please visit:
https://www.microsoft.com/en-us/trustcenter/cloudservices/azure

For optimal accessibility and additional security of our Blue10 service, we use Azure Front Door as a Content Delivery Network (CDN) and its inherent Intelligent Network Threat Protection.

6. Security Operations Center (SOC)

Blue10 uses the services of a reputable and specialized third-party Security Operations Centre (SOC). The SOC continuously monitors our systems and network for suspicious events (*security incident & event monitoring (SIEM)*) or anomalies that could be an indication of security problems or vulnerabilities. It informs us about them and assists in analysis and resolution. The choice to use an external SOC is deliberate. Today's (cyber) threat landscape is so dynamic and complex that specialized knowledge is required to be properly armed against it.

7. Logical access security

We only grant access to information in the Blue10 systems to employees who need this access because of their role and function in our organization (role based access). In doing so, we distinguish between rights to amend information and rights to view information. Where possible, we use automated tools to enforce authentication or authorization (such as Azure Active Directory and Azure Role Based Access (RBAC).

When employees change positions within Blue10 or leave the organization, their rights will be, respectively adjusted or revoked.

We heavily rely on measurements enforced by Azure Active Directory for *identity management* and authentication. We strictly distinguish between the office side, within which Blue10 employees can use office applications, and the production side within which our Blue10 service is offered. Situations may arise where, temporarily or otherwise, certain rights need to be granted to administrators in the context of problem solving or incident handling. We use Microsoft's Privileged Identity Management for this, which ensures a controlled, temporary, and auditable allocation of rights.

We store customer data in separate environments within the Blue10 architecture, namely a customer-specific container in Azure object storage (Blob) and a customer-specific database within a connection pool of SQL Server. This contributes to a logical separation of customer environments and reduces the risk of unauthorized access.

8. Physical access security

Blue10 works in an office environment in The Hague. Because of our cloud philosophy and the absence of an on-site infrastructure, in combination with our clear screen/ clean desk-policy and encryption of all endpoints such as laptops for instance, the risk of physical access to devices or media with information is minimal. Nevertheless, we also have in-house physical access protocols in place to warrant any unauthorized access, such as department zoning, employee & visitor badges, card readers, alarms and a visitor intake protocol at our building reception.
For the physical security of our infrastructure in Microsoft data centers, we rely on the measures taken by Microsoft. Naturally, we take note of assurance reports and certifications demonstrating the quality of these measures.

9. Endpoint security

From a security perspective, Blue10 applies the principle that customer data is not stored on endpoints (laptops, workstations, mobile devices). Storage of other data on these endpoints is encrypted using BitLocker. Blue10 monitors and detects malware and vulnerabilities on endpoints by using products such as Intune and Microsoft Defender. New endpoints are provided with an approved, standard configuration. Deviations from this configuration are detected and followed up. The use of USB-sticks are forbidden and been made technically impossible to access.

10. Encryption

Customer data is stored in Azure object storage (Blob) and SQL Server databases. The data are encrypted 'at rest', with encryption management performed by Microsoft. The connection between the customer environment and the Blue10-service ('data in transit') is encrypted with TLS 1.2. These encryption measures ensure data confidentiality.

11. Logging and monitoring

The logging of relevant systematic events is important for handling incidents, detecting anomalies and for checking performed tasks. Blue10 uses Azure facilities for this purpose, in particular Log Analytics workspaces and Sentinel (cloud-native SIEM). Log files in Azure Log Analytics are retained for two years.

Blue10 uses the extensive functionalities, dashboards and metrics from Microsoft Azure for monitoring the system resources and performance. These provide continuous insight into the performance of our service and give alerts the moment previously predefined thresholds are reached. This allows timely action the be taken if problems regarding to the 'health' of our service are imminent. Examples of key processes that are continuously monitored within the Blue10 service are:

- Availability infrastructure
- Average response time website
- Response time from a login request
- Lead time per page from entrance to conversion
- Lead time from recognition process per page
- Response time between the Blue10 service and the difference accountancy systems

12. Back-up & Restore

All databases run on the SQL Azure Platform. This platform offers built-in redundancy, back-up and restore capabilities. Blue10 distinguishes between two types of back-ups:

1. Blue10 creates full, point-in-time back-ups on Microsoft Azure that are saved for a period of 7 days. This means that, if necessary, we can restore a situation as it was at any given moment in the past seven days.
2. In addition, Blue10 creates a back-up once a week on Microsoft Azure that is saved for a period of 8 weeks.

Azure Blob Storage is used for storing files. This service offers unlimited scalability and built-in redundancy. When deleting files in Blob, soft delete is used. This means that files are recoverable up to 30 days after deletion.

13. Development

Blue10 focuses strongly on the maintenance and development of the Blue10 service. Blue10 designs and builds the software in-house and, by doing so, maintains maximum control over the quality of the development. New releases within Blue10 are made available to our customers through a process of continuous delivery, but not before a careful development and change management process has been completed. We use solid development standards, an elaborate range of tests (unit, component, load and regression tests), peer reviews and automated supportive quality controls on the coding that consist of accepted security principles. The entire development and deployment trajectory is supported and facilitated by Azure DevOps.

14. Penetration testing

At least once a year, Blue10 has a penetration test performed on its service's application infrastructure. This penetration test is performed by an independent and specialized external party, which then reports any existing vulnerabilities in our security and advises on measures to be taken for improvement. Blue10 actively follows up on these findings from the penetration test (and review).

15. Assurance

Increasingly, organizations are expected to demonstrate and make evident that they are in and have full control of their activities. Understandably for any company to ensure and verify their security measures of their internal processes may pose a huge challenge. This challenge is enlarged or multiplied when certain services or processes are outsourced, for instance to an organization such as Blue10. Customers count on security, availability and integrity of these external services and look for assurance that the quality is guaranteed.

At Blue10 we believe in the quality of our services and we think it is important that we can also demonstrate that quality to our customers. A 'security and privacy white paper' such as this document is not sufficient for this. That is why in addition to this document, we annually issue two assurance reports on our internal control and information security. These reports (according to ISAE 3402 and the SOC2 standard respectively) describe our services and the measures we have taken to ensure control of the Blue10 service. An independent (registered) IT auditor tests and assesses whether this description corresponds to reality and whether the described measures have actually been implemented and function properly. With these reports, we help our customers to verify that they are also 'in control' for the activities they outsource to Blue10. More crucially we highly value our ability to make evident and deliver the necessary certainty, reliability and quality of our services with these assurance reports and that this provides a trustworthy solid foundation for choosing Blue10 as a preferred service provider and partner.

Current clients, prospective clients (and their auditors) are welcomed to read the most recent assurance reports. For more information please visit: https://www.blue10.com/en/certifications-blue10/

16. Data Pro code

In terms of privacy, especially in the role of a processor, Blue10 conforms to the Data Pro Code. This is a code of conduct drawn up by NL Digital, the industry association of IT companies, and approved by the Personal Data Authority (Autoriteit Persoonsgegevens). After an independent audit, we are certified annually for complying to this code of conduct, which indicates that we handle personal data entrusted to us by customers for processing with care and in line with the AVG. This is reflected in the provision and conclusion of processor agreements, internal overview by our Data Protection Officer and a structured process of the correct handling of any potential data leaks.

17. Responsible disclosure

At Blue10, we find the security of our systems, our network and our products very important. Despite taking great care of our information security, it may occur that a weak spot is discovered. When a vulnerability is discovered by a third party (not being Blue10 employees, clients, or suppliers), Blue10 has a Responsible Disclosure policy, in which we make arrangements with reporters of vulnerabilities and commit to resolving any issues seriously and promptly. Our responsible disclosure policy can be found here: https://www.blue10.com/en/responsible-disclosure-blue10/

18. What do we expect from our customers?

Despite the efforts that Blue10 takes in terms of information security and privacy, a safe and responsible use of the Blue10 service is also dependent of a number of measures that our customers are responsible for themselves.

A sufficient IT infrastructure
Make provisions of modern work stations and laptops for employees who use the Blue10 service, with a modern browser that is up-to-date. Naturally, the availability of a functioning and stable internet connection is essential for using Blue10.

A choice for an authentication method that fits the information security policy
Blue10 offers multiple possibilities for users to log into the Blue10 service, varying from 'normal' combinations of username and password to a link with identity management in an existing Microsoft Azure Directory.

A careful handling of authentication information.
To prevent unauthorized access and unauthorized bookings, the customer has to make sure that authentication information (like username and password) are maintained confidential, and are renewed in line with their own policy.

Careful user management.
Customers themselves manage authorized users and their rights in the Blue10 service. It is important that they align and maintain these with their own administrative organization and internal control requirements in terms of authorizations and segregation of duties.

An adequate validation process.
Although the Blue10 service provides a proposal of recognized values of an invoice and a corresponding coding and/or booking proposal, it is the customer's responsibility to check, validate, and authorize such a proposal. The accuracy of the processed data is and remains a responsibility of the customer.

Solid master data management.
Master data management is essential in an administrative environment, as incorrect master data can cause various errors later in the organization's administrative processing. The Blue10 service relies significantly on that master data, and hence also on the quality of processes to ensure the accuracy of master data.

Provision of information.
To respond properly and quickly to any malfunctions and problems in the use of our service, we count on our customers to inform us of any problems they encounter. Feedback on our service or suggestions for improvement are highly appreciated and proactively followed up.