BitaBIZ Policies

(01 October 2020)

Content

1 Information Security Policy

BitaBIZ is committed to preserving the confidentiality, integrity, and availability of all the physical and electronic information assets throughout our organization and we continuously seek to improve the protection of our customers.

The purpose of this policy is to ensure that BitaBIZ will apply a consistent, business risk based and coast efficient approach in order to manage information security.

BitaBIZ will identify and manage risks to information, applications, and technology applying Information Security Management System (ISMS) intended to follow and conform to the best practice standards. Protecting information assets addresses all stocks of information, the network, the people that use them, the processes they follow, and the physical computer equipment used to access them.

This policy applies to BitaBIZ management, all full time or part-time employees, sub-contractors, project consultants, any other person who works under the authority of BitaBIZ and any external party.

This policy describes:

1.1 Network and Application Security
Measures implemented to prevent unauthorized access, use, alteration or disclosure of customer data.

1.2 Product Security
Measures implemented to secure data portability, privacy by design, access management and password security.

1.3 Internal Security
Measures implemented to educate our employees.

1.1 Network and Application Security

Data Hosting and Storage
BitaBIZ service and data are hosted at Microsoft Azure in the EU. We do not run our own routers, load balancers, DNS servers, or physical servers.

Security
Cloudflare

Our Azure Cloud Services and Virtual Machines is protected by Cloudflare web application firewall (WAF). BitaBIZ is protected against all-important safety risks. BitaBIZ WAF is certified by the PCI Security Standards Council.

All data sent to or from BitaBIZ is encrypted in transit using 256-bit encryption. Our API and application endpoints are TLS only. We automatically use the newest TLS version when supported by the clients.

BitaBIZ is HSTS (HTTP Strict Transport Security) enabled and all requests are forced to use https.

Microsoft Azure
BitaBIZ Azure databases are encrypted with Encryption-at-rest by default and the database encryption key is protected by a built-in server certificate.

Microsoft Antimalware is installed on our Azure Cloud Services and Virtual Machines.

Login to our production environment is only via Microsoft Azure Just-in-Time that provide audit logs for all activity.

Data retention: Point in time backups are stored for at least 1 month back, and monthly backups are stored for at least 6 months.

BitaBIZ is delivered via Microsoft .NET technology platform. Our Microsoft resources like MS SQL are always updated with the latest security updates.

Platform Monitoring, Penetration Tests and Vulnerability Scanning
BitaBIZ uses Rapit7 to continuously scan for vulnerabilities. This enables us to identify and remove vulnerabilities.

BitaBIZ uses New Relic real-time platform monitoring. This enables us to monitor performance and quickly identify errors.

1.2 Product Security

SAML 2.0
Single Sign-on (SSO) allows your company to authenticate users in your own systems without requiring them to enter login credentials to BitaBIZ.

Manual Password and Credential Storage
Password-based authentication; user passwords are encrypted using the protocol SHA1 or later version.

Authentication Controls

Measures are implemented to restrict number of login attempts.

Session timeout

Sessions timeout is implemented.

SCIM

User provisioning allows your company to control and manage user creation and access control from your own systems.

User Role Permissions (Privacy by Design)

BitaBIZ has built-in settings and permission management.

Permission roles include:

- System admin
- Global payroll admin
- Local Payroll admin
- External admin
- HR statistics
- Approver role
- User role

Settings management:

- Default settings
- GDPR setting
- User settings

Data Portability and Data Management

BitaBIZ has built-in tools that allow the customer to respond to employee requests to delete personal information if the information is no longer relevant.

1.3 Internal security

Training

All our employees have received security awareness training and more specialized staff have received appropriately specialized information security training.

Policies

Our setup does not allow our staff to access business resources outside our implemented Information Security Policy.

Employee Vetting

BitaBIZ performs background checks on all new employees including employment verification and criminal checks for Danish employees.

Confidentiality

All employee contracts, consulting agreements, vendor agreements, or service delivery agreements include confidentiality clauses to set forth a duty of secrecy and security of customer data and personal data even after the engagement with BitaBIZ ends.

Internal permissions and authentication

- Access to customer data is limited to authorized employees who require it for their job.
- BitaBIZ has a Single Sign-On (SSO) policy for all business resources. SSO is a requirement for implementing a business resource. We manage resource access from one central portal. Access to a resource is only granted if relevant for the job function.
- We monitor and audit log login to all company resources.
- All actions taken on production consoles are logged.
- We have strong password policies.

Audit

BitaBIZ employees must enable and contribute to audits, including inspections carried out by our customers or another auditor that has been authorized by the customer.

Hardware

All employees have company paid PC and Mobile secured with company managed firewall and security scan.

PCs are wiped every year. Data must only be saved on company managed SharePoint/OneDrive.

As a part of the overall security management, BitaBIZ assesses the Information Security Policy annually.

BitaBIZ Information Security Policy accompanies BitaBIZ Terms & Conditions (System2 25.05.2018).

2 Sub-processor policy

BitaBIZ engages selected sub-processors that may process personal data submitted to BitaBIZ services.

A BitaBIZ sub-processor must meet and comply with EU GDPR regulation regarding the processing of personal data as specified in Article 28 of the GDPR.

If the sub-processor processes personal data outside the EEA, the processing may take place only in full compliance with Chapter V of the GDPR.

Adequacy decision. Personal data may flow outside the EEA if European Commission has decided that the third country or an international organization ensures an adequate level of protection of personal data.

In absence of adequacy decision, the sub-processor must provide appropriate safeguards that include binding on the sub-processor:

- A legally binding and enforceable instrument between public authorities or bodies.
- Binding Corporate Rules approved by the competent supervisory authority
- Standard Contractual Clauses (SCCs) approved by the European Commission
- Approved Codes of Conduct
- Approved certification mechanisms

Statement. BitaBIZ does not rely on the EU-U.S. Privacy Shield Framework as a legal basis for transfers of personal data to the USA. Nonetheless, if the sub-processor is processing data in the USA, the sub-processor must comply with EU-U.S. and Swiss-U.S. Privacy Shield Framework and adhere to the security standards they entail.

Sub-processors used by BitaBIZ are listed below. The list may be updated by BitaBIZ from time to time:

Sub-processor	Purpose of using the sub-processor	Place of data processing	Note
Intercom	Online support	USA	GDPR compliant DPA with incorporated SCCs approved by the EU Commission SOC 2 certification EU-U.S. and Swiss-U.S. Privacy Shield framework
Microsoft AZURE	Hosting	EU	EU-U.S. and Swiss-U.S. Privacy Shield framework
Twilio/SendGrid	E-mail gateway	USA & EU	Twilio's binding corporate rules at Link SCCs approved by the EU Commission SOC 2 certification EU-U.S. and Swiss-U.S. Privacy Shield framework
New Relic	Infrastructure monitoring	USA & EU	GDPR compliant DPA and SCCs approved by the EU Commission SOC 2 certification EU-U.S. and Swiss-U.S. Privacy Shield framework
Cloudflare	Traffic optimization and Web application firewall (WAF)	USA & EU	GDPR compliant DPA and SCCs approved by the EU Commission PCI DSS certified EU-U.S. and Swiss-U.S. Privacy Shield framework
Link Mobility	SMS-gateway	EU	GDPR compliant DPA IASE 3402 Type II certified
Rapid7	Vulnerability scanning	EU	GDPR compliant DPA SOC 2 certification Certified under the EU-U.S. Privacy Shield Framework

BitaBIZ Sub Processor Policy accompanies BitaBIZ Data Processing Agreement part of BitaBIZ Terms & Conditions (System2 25.05.2018).

3 Support policy

- Access to online support is provided 24 hours per day, 7 days per week.
- BitaBIZ response to support requests is delivered within normal business hours. 8.00 pm – 17.00 am (CET / GMT +1).
- Online support is available to customers and non-paying customers.
- Support services include setting up customer accounts.
- Target response time within normal business hours on a support request is 15 minutes.
- BitaBIZ support agents are instructed not to offer support related to internal company policies. And not to receive personal data like password or payroll related information.

BitaBIZ Support Policy accompanies BitaBIZ Terms & Conditions (System2 25.05.2018).

4 Pricing policy

We invoice based on:

1. the BitaBIZ modules activated to your subscription,
2. the number of employees (active users*) added to your BitaBIZ account,
3. the number of SMS messages** sent,

These are the "Pricing Metrics" that are used to calculate your invoice. We invoice each quarter in advance based on what your Pricing Metrics were on the last day of that quarter.

Payment deadline from invoice date 14 days.

*Inactive users are not part of the "Pricing Metrics". History/ data on inactive users can be saved or deleted according to local legislation requirements.

**SMS messages are invoiced based on actual consumption in the previous quarter.

The customer has access to manage the "Pricing Metrics" by activating or deactivating modules and users.

Subscription remuneration indexed by DST published in January. The amendment regulates subscription remuneration from the nearest following 1. April.

BitaBIZ Pricing Policy accompanies BitaBIZ Terms & Conditions (System2 25.05.2018).

5 Data collect policy

BitaBIZ account registration and contact information.

We collect information when an account is registered with the intent to use or test our services.

The information you provide includes: first and last name, company name, department, e-mail address, preferred account settings.
You may also provide us your phone number and billing information.

Data you may choose to pro using our service.

You may submit various types of information and data into our services for hosting and processing purposes. Data may include:

Personal data that can be registered in BitaBIZ:

- The employee name
- E-mail
- Phone number
- Hiring/ termination date
- Date of birth
- Private address
- Department
- Manager / approver
- Private car registration no.
- Employee & salary no.
- Tags
- Collective agreement
- Employee documents

Types of registrations that can be registered on an employee in BitaBIZ:

- Vacation
- Sick days
- Time off & overtime
- Custom leave types
- Custom event types
- Time registrations
- Mileage registrations

BitaBIZ Data Collect Policy accompanies BitaBIZ Terms & Conditions (System2 25.05.2018).

6 Cookie Policy for bitabiz.com (the Service)

Our Cookie policy explains what cookies are, which cookies do we use and why, and how do we use cookies.

What are cookies?

Cookies are small pieces of data stored on your computer by the web browser. Cookies usually remember your personal or website settings. When you visit our website, your browser returns these pieces of data to us that help us to make this site and our Service work properly.

However, you can allow or prohibit cookie requests or delete stored cookies by changing the settings on your browser.

Our Cookie policy for our Service is:

- We use first-party and third-party cookies.
- We only use cookies if required for technical reasons in order for our Service and platform to operate.
- We only use cookies we see as "strictly necessary".

This is described in more detail below.

How is BitaBIZ using cookies?

We use cookies to recognize you when you visit our Service, remember your preferences, and give you a personalized experience that's consistent with your settings.

Cookies we use also make your interaction with our Service faster and more secure.

The different categories of cookies we use

Categories of Use	Description
Authentication	If you're signed into our Service, cookies help us show you the right information.
Security	We use cookies to enable and support our security features.
Preferences, features and services	Cookies can tell us which language you prefer and which settings you last used on the team calendar.
Marketing	We do not use any cookies for marketing purposes on our domain bitabiz.com (our Service).

Categories of Use	Description
	We do use marketing cookies on our domain bitabiz.dk (our marketing website. Please see our cookie policy for our domain bitabiz.dk for more information regarding this) On our bitabiz.com domain, we use cookies to remove customers from marketing campaigns. These cookies remove the user from marketing campaigns targeted at marketing website visitors.
Performance, Analytics and Research	Cookies help us learn how well our Service performs. We also use cookies to understand and improve our Service.

Our cookie table for our Service (bitabiz.com)

The table provides our cookie list. The list offers transparency into the cookies and similar technologies we use to deliver our service.

The following are first-party cookies used on bitabiz.com:

Domain	Cookie Name	Expiration	Description
bitabiz.com	caltype	Session	Calendar setting for month/ week / day view
bitabiz.com	bitabiz	Session	Storing of language preference
bitabiz.com	BitabizAuthCookie	1 week	Authorization
bitabiz.com	ASP.NET_SessionId	Session	.net session

The following are third-party cookies used on bitabiz.com:

Domain	Cookie Name	Expiration	Description
bitabiz.com	cfduid	1 year	Cloudflare. The __cfduid cookie is used to identify individual clients behind a shared IP address and apply security settings on a per-client basis.
bitabiz.com	utma	2 years	Google analytics to distinguish visitors
bitabiz.com	utmb	30 min	Google analytics to determine new visits
bitabiz.com	utmc	session	Google analytics
bitabiz.com	utmz	6 months	Google analytics for traffic source or campaign

bitabiz.com	ga	2 years	Google analytics to distinguish users
bitabiz.com	gid	24 hours	Google analytics to distinguish users
bitabiz.com	intercom-lou-	9 months	Intercom for identifying visitors
bitabiz.com	intercom-session-	1 week	Intercom session cookie
addin.bitabiz.com	MicrosoftApplications TelemetryDeviceId	1 year	Addin / Microsoft Graph API
addin.bitabiz.com	MicrosoftApplications TelemetryFirstLaunchTime	1 year	Addin / Microsoft Graph API

BitaBIZ Cookie Policy accompanies BitaBIZ Terms & Conditions (System2 25.05.2018).

7 Service Level Agreement

1. **Target Availability.** BitaBIZ will use commercially reasonable efforts to make our service available with an uptime of 99.8% of each calendar month ("Target Availability").
2. **Scheduled Maintenance.** "Scheduled Maintenance" means BitaBIZ scheduled routine maintenance of the platform. Scheduled Maintenance will not exceed (8) hours per month. BitaBIZ typically performs Scheduled Maintenance each week. After 9 am (CET +GMT).
3. **Exclusions.** The calculation of uptime will not include unavailability to the extent due to: (a) use of the service by customer in a manner not authorized in this Agreement or the applicable Documentation; (b) general Internet problems, force majeure events or other factors outside of BitaBIZ reasonable control; (c) customer's equipment, software, network connections or other infrastructure; (d) third party systems, acts or omissions; or (e) Scheduled Maintenance or reasonable emergency maintenance.
4. **Scheduled maintenance and downtime** are published on the BitaBIZ status page: https://status.bitabiz.com/.

BitaBIZ Service Level Agreement accompanies BitaBIZ Terms & Conditions (System2 25.05.2018).

8 Data Protection & Privacy Policy

Introduction

BitaBIZ needs to collect and use certain information about individuals to carry out our business activities. These can include customers, suppliers, business contacts, employees, and other people we have a relationship with or may need to contact.

BitaBIZ is committed to protecting the personal data of our employees, users of our services, contractors, and website visitors. This policy is applicable in situations where we act as a data controller or data processor with respect to this personal data.

This policy describes how this personal data must be collected, handled and stored to meet our data protection standards and to comply with the Regulation (EU) 2016/679 (General Data Protection Regulation) referred to as "**the GDPR**".

In this document, "we", "us", and "our" refer to BitaBIZ.

Purpose

The purpose of this policy is to protect and promote the data protection rights by informing everyone working for BitaBIZ and any third party to whom this policy applies to of their data protection obligations and of the BitaBIZ procedures that must be followed to ensure compliance with the GDPR.

Scope

This Privacy Policy applies to BitaBIZ online platform (bitabiz.com), including the associated BitaBIZ mobile apps, Outlook app and Win10 app (collectively, the **"BitaBIZ Service"**), and other interactions (e.g., customer service inquiries, user conferences, etc.) you may have with BitaBIZ.

All BitaBIZ employees, contractors, consultants, freelancers, and any other person who works under the authority of BitaBIZ must comply with this policy, including all personnel affiliated with third parties who may have access to any BitaBIZ network or resource.

This policy applies to BitaBIZ processing of personal data, whether by electronic or manual means.

Privacy Principles

The following sets out the principles that underline our practices for collecting, using, disclosing, storing, securing, accessing, transferring, or otherwise processing personal data.

Fairness. BitaBIZ shall process personal data in a lawful, legitimate, and transparent manner.

Purpose Limitation. BitaBIZ shall only collect personal data for specific, explicit, and legitimate purposes.

Proportionality. BitaBIZ shall only process personal data that is adequate, relevant, and not excessive for the purposes which it is processed.

Data Integrity. BitaBIZ shall keep personal data that is accurate, complete, and up to date, as is reasonably necessary to accomplish the purpose for which it is processed.

Data Retention. BitaBIZ shall keep personal data in a form that is personally identifiable for no longer than necessary to accomplish the purpose for which the personal data was obtained unless required by law to retain some information for a period of time.

Data Security. BitaBIZ shall implement appropriate and reasonable technical and organizational measures to safeguard personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, use, and access.

Individual Rights. BitaBIZ shall process personal data in a manner that respects individuals' rights as required by the GDPR.

Accountability. BitaBIZ shall implement appropriate governance, policies, processes, controls, and other measures necessary to demonstrate that it processes personal data following this policy and the GDPR.

Legal Basis for Processing Customer and Partner Data

Data processing for contractual relationship. Personal data of the customer or partner can be processed to establish, perform, and terminate a contract.

Consent to data processing. Personal data can also be processed following the consent by the data subject. Before giving consent, the data subject must be informed. The declaration of consent must be obtained in writing or electronically for the purposes of documentation.

Legal authorization or obligation. The processing of personal data is permitted if national legislation requests, requires, or permits this. The type and extent of processing must be necessary for the legally authorized data processing activity and must comply with the relevant statutory provisions.

Legitimate Interest. Personal data can also be processed if necessary, for legitimate interests (e.g., avoiding breaching of contract). Before data is processed, it is needed to determine whether the data subjects' interests worthy of protection outweigh the legitimate interests.

Employment relationship. Personal data can be processed if needed to establish, perform, and terminate the employment relationship. In the existing employment relationship, data processing must always relate to the purpose of the employment. Personal data of candidates can be processed to help to decide whether to enter into an employment relationship. If the candidate is rejected, their data must be deleted, unless the candidate has agreed to remain file for future selection process.

Personal Data We Collect and Receive

BitaBIZ collects and receives customer data. Below are the kinds of data we collect and reasons for doing so. We do not use this data for other purposes.

1. When a BitaBIZ account is created, the following information may be collected:

- **User data**. Users (employees) or individuals granted access to a BitaBIZ account by a customer ("**Setup Admin user**") routinely submit customer data to BitaBIZ when using the Services. Data like vacation requests, time registrations, sick leave registrations, etc.
- **Customer data.** BitaBIZ is also used to collect other customer data. To create or update a BitaBIZ account, you or your employer supply BitaBIZ with an email address, phone number and other staff/ HR/ payroll related information.
- **Billing information**. Customers that purchase a paid version of the BitaBIZ Services provide BitaBIZ (or its payment processors) with billing details such as credit card information, banking information and/or a billing address.

Our Data Collect Policy describes in detail what data may be collected using the BitaBIZ service. Click here to read our Data Collect Policy.

2. BitaBIZ also collects, generates, and/or receives other information:

- **Cookie information**. BitaBIZ uses cookies and similar technologies on our websites and services.
- **Device information**. BitaBIZ collects information about devices accessing the services, including the type of device and what operating system is used.
- **Logs**. Our servers automatically collect information when you access or use our services and record it in log files. This log data may include the Internet protocol (IP) address.

  Click here to read our Cookie policy.

How We Use Information

The information added to BitaBIZ will be used in accordance with the Customer's instructions. BitaBIZ is a processor of Customer Data and the Customer is the controller. The Data Processor Agreement (DPA) govern how BitaBIZ shall act as the data processor. Click here to read the DPA.

Where We Store and Process Personal Data

BitaBIZ is hosted in a cloud and data we collect is stored in the Microsoft Azure platform. Microsoft enterprise cloud services are independently validated through certifications and attestations, as well as third-party audits. In-scope services within the Microsoft Cloud meet key international and industry-specific compliance standards, such as ISO/IEC 27001 and ISO/IEC 27018, FedRAMP, and SOC 1 and SOC 2. They also meet regional and country-specific standards and contractual commitments, including the EU Model Clauses, UK G-Cloud, Singapore MTCS, and Australia CCSL (IRAP). In addition, rigorous third-party audits, such as by the British Standards Institution and Deloitte, validate the adherence of their cloud services to the strict requirements these standards mandate.

Microsoft has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. Microsoft has stated that it and its controlled U.S. subsidiaries (collectively "Microsoft") will continue to comply with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce.

Data Subject's Rights

A data subject has the following rights vis-à-vis the controller:

- The right to be informed of the circumstances in the processing of their personal data (Right of transparent communication and information)
- The right obtain information about how their data is processed and what rights they are entitled to in this respect (Right of access).
- The right to correct or supplement personal data if data are incorrect or incomplete (Right to rectification).
- The right to delete their personal data if the legal bases has ceased to apply. Existing retention periods and interests worthy of protection that prohibit deletion must be observed (Right to erasure).
- The right to restriction of processing if they dispute the accuracy of processing or the controller no longer needs the data while the data subject needs the data for their legal claims (Right to restriction of processing).
- The right to receive their personal data which has provided on the bases on a consent or in context in the agreement initiated by them in a commonly used digital format. Data subject has also the right to transfer this data to a third party (Right to data portability).
- The right to object to direct marketing at any time (Right to object).
- Right not to be subject to automated decision-making.
- The right to lodge a compliant

Access to Your Data

All individuals who are the subject of personal data held by BitaBIZ are entitled to:

- Ask what information BitaBIZ holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up-to-date.

- Be informed how the companies meeting its data protection obligations.
- Request removal

Security

Our Information Security Policy describes our:

- Hosting security
- Product security
- Internal security

Click here to read our Information Security Policy

International Data Transfers

BitaBIZ may transfer personal data added to the BitaBIZ services to countries other than the one in which you live.

BitaBIZ has an EU GDPR compliant data transfer setup:

- data storage inside the EU
- engages only selected sub-processors that may process personal data submitted to BitaBIZ services.

Click here to read our Sub-processor Policy.

Customers' Rights

BitaBIZ customers have statutory rights in relation to data stored on the BitaBIZ service.

BitaBIZ provides data management tools to manage and delete personal data according to local law. If you cannot use the settings and tools, contact BitaBIZ online support for assistance.

Your rights to your data stored on the BitaBIZ service is described in our Terms & Conditions.

Contacting BitaBIZ

Please also feel free to contact BitaBIZ if you have any questions about this Data Protection & Privacy Policy or if you are seeking to exercise any of your statutory rights. You may contact BitaBIZ at bitabiz@bitabiz.com or via online support.

Complaints

If you want to lodge a complaint over our processing of your personal data, please contact us directly. If we cannot help you, you can lodge a complaint to the national Data Protection Authority.

Definitions

Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Data controller	Is the one who determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Data processor	Is the one who processes personal data on behalf of the controller.
Personal data processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

BitaBIZ Data Protection and Privacy Policy accompanies BitaBIZ Terms & Conditions (System2 25.05.2018)