ProfitWell is the world's leading provider of subscription analytics, pricing, and retention software. Over ten thousand companies in more than 50 countries use ProfitWell's software, services, and support to change the way they view and grow their recurring revenue businesses.

ProfitWell's primary security focus is to safeguard our customers' and users' data, which is why ProfitWell has invested in the proper resources and controls to protect and service our customers. Our investment in security and privacy utilizes a security framework using best practices in the SaaS industry with our key objectives centering on:

1. Data privacy and safety: Deliver a superior product and service to our users and customers while protecting the privacy and confidentiality of their data
2. Service continuity: Maintain ongoing availability of ProfitWell and data to all authorized individuals
3. Data and Service Integrity: Ensure that user and customer data is never corrupted or altered inappropriately
4. Compliance and Best Practices: Implement process and controls to align with current international regulatory and industry best practice guidance

ProfitWell values transparency when it comes to security and privacy to the extent that we can be without opening us up to vulnerabilities. This document is designed with that transparency in mind. We are continuously improving the protections that have been implemented and, along those lines, the information and data in this document is consistently being updated.

If you'd like more detail or wish to complete a security and risk assessment, email Product@ProfitWell.com to get routed to the appropriate person.

Security and Privacy at a Glance

Our success hinges on providing a safe and trustworthy environment for your subscription data. Protecting your data is our obsession, which involves a cross-functional approach with initiatives big and small. Here's an overview of the major themes of our privacy and security protocols.

Data Privacy and Use

- ***Data is never sold and rarely accessed:*** Your data is your data and will never be sold to third parties. Further, your data is only accessed with permission or in the event of a security or QA issue.
- ***Data is studied in aggregate:*** Data is studied in aggregate to improve our products, security, and knowledge of the market. You can easily opt out of this through a custom Terms of Use.
- ***GDPR Compliant:*** ProfitWell maintains compliance with the EU's General Data Protection Regulation and maintains product features, corporate protocols, and legal documents to help our users and customers comply.
- ***EU-US and Swiss-US Privacy Shield Certification:*** ProfitWell certified it's compliance with the EU-US and Swiss-US Privacy Shield framework.

Resiliency and Availability

- ***99.999% Uptime:*** ProfitWell's availability is consistently above 99.999%. Customer data is 100% backed up to multiple online replicas with additional snapshots.
- ***24x7x365 Monitoring:*** Our product and operations team monitor application, software, and infrastructure behavior using proprietary and industry recognized solutions.
- ***Data Center Redundancy:*** ProfitWell maintains multiple failover instances to prevent outages from single points of failure.

Application and Software Security

- ***Data Encrypted in Transit:*** Data sessions are always protected with advanced TLS protocols and 2,048-bit keys.
- ***Security incorporated into the SDLC:*** ProfitWell code is high quality from conception to deploy. We use code analysis to ensure best practices are implemented directly into the software development lifecycle (SDLC).
- ***Responsive incident response program:*** ProfitWell's incident response program process flows and investigation data sources utilize standard incident response process structures to ensure that the right steps are taken in the event of a vulnerability.

Data Centers and Network Security

- ***Utilize leading, compliant data centers:*** ProfitWell products are hosted with the world's leading data center providers. Access to these data centers is strictly controlled. These partners are SOC 2 Type II and ISO 27001 certified and provide N+1 redundancy to all power, network, and HVAC services
- ***Diverse data center infrastructure:*** ProfitWell infrastructure is distributed to ensure that single failure does not impact our users and customers.
- ***Network firewall protection:*** ProfitWell prevents network attacks with monitoring and protections including tightly controlled network-level firewalling.

Audits and Penetration Testing

- ***3rd-Party Network Penetration Testing:*** ProfitWell utilizes industry-respected 3rd party penetration testing firms 2 times per year to test our network, product, and corporate infrastructure.
- ***3rd-Party Physical Penetration Testing:*** Once per year, ProfitWell utilizes industry-respected 3rd party penetration testing firms to test our physical office security.
- ***Numerous external audits and assessments:*** ProfitWell certified with the EU-US and Swiss-US Privacy Shield Framework. Our data center providers maintain ISO 27001, SOC2 Type II, and many other certifications. We also maintain numerous security questionnaires from our vendors on file, including Google's VSAQ

If you'd like access to our full security, privacy, and risk assessment, email.....

SECURITY

1. Personnel. ProfitWell's personnel will not process customer data without authorization. Personnel are obligated to maintain the confidentiality of any customer data and this obligation continues even after their engagement ends.

2. Data Privacy Contact

200OK, LLC
Attn: Michael Cox - ProfitWell
109 Kingston Street (4th Floor)
Boston, MA 02111

3. Technical and Organization Measures. ProfitWell has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect your customer data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows:

3.1 Organization of Information Security. ProfitWell has appointed Michael Cox as the security officer responsible for coordinating and monitoring the security rules and procedures. ProfitWell's personnel with access to customer data are subject to confidentiality obligations.

3.2 Risk Management. ProfitWell conducts regular testing and monitoring of the effectiveness of its safeguards, controls, systems, including conducting penetration testing. ProfitWell implements measures, as needed, to address vulnerabilities discovered in a timely manner.

3.3 Storage. ProfitWell's database servers are hosted in a data center operated by a third party vendor, that has been qualified per ProfitWell's vendor management procedure. ProfitWell maintains complete administrative control over the virtual servers, and no third-party vendors have logical access to customer data.

3.4 Asset Management.

a. **Asset Inventory.** ProfitWell maintains an inventory of all media on which customer data is stored. Access to the inventories of such media is restricted to authorized personnel.

b. **Asset Handling.** ProfitWell employees are required to utilize encryption to store data in a secure manner and are required to use two-factor authentication to access 200OK, LLC's networks. ProfitWell imposes restrictions on printing customer data and has procedures for disposing of printed materials that contain customer data. Personnel must obtain authorization prior to storing customer data on portable devices, remotely accessing customer data, or processing customer data outside ProfitWell's facilities.

3.5 Software Development and Acquisition. For the software developed by ProfitWell, the company follows secure coding standards and procedures set out in its standard operating procedures.

3.6 Change Management. ProfitWell implements documented change management procedures that provide a consistent approach for controlling, implementing, and documenting changes (including emergency changes) for ProfitWell's software, information systems or network architecture. These change management procedures include appropriate segregation of duties.

3.7 Third Party Provider Management. In selecting third party providers who may gain access to, store, transmit or use customer data, ProfitWell conducts a quality and security assessment pursuant to the provisions of its standard operating procedures.

3.8 Human Resources Security. ProfitWell informs its personnel about relevant security procedures and their respective roles, as well as of possible consequences of breaching the security rules and procedures. Such consequences include disciplinary and/or legal action.

3.9 Physical and Environmental Security.

a. **Physical Access to Facilities.** ProfitWell limits access to facilities where information systems that process customer data are located to identified authorized individuals who require such access for the performance of their job function. ProfitWell terminates the physical access of individuals promptly following the date of the termination of their employment or services or their transfer to a role no longer requiring access to customer data.

b. **Physical Access to Components.** ProfitWell maintains records of the incoming and outgoing media containing customer data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of customer data they contain.

c. **Protection from Disruptions.** ProfitWell uses commercially reasonable systems and measures to protect against loss of data due to power supply failure or line interference.

d. **Component Disposal.** ProfitWell uses commercially reasonable processes to delete customer data when it is no longer needed.

3.10 Communications and Operations Management.

a. Security Documents. ProfitWell maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel.

b. Data Recovery Procedures. On an ongoing basis, ProfitWell maintains multiple copies of customer data from which it can be recovered and stores copies of customer data and a data recovery procedures in a different place from where the primary computer equipment processing the customer data is located. ProfitWell has procedures in place governing access to copies of customer data as well as anti-malware controls to help avoid malicious software gaining unauthorized access to customer data.

c. Encryption; Mobile Media. ProfitWell uses HTTPS encryption on all data connections and restricts access to customer data in media leaving its facilities.

d. Event Logging. ProfitWell logs the use of our data-processing systems and we maintain logs for at least 30 days.

3.11 Access Control.

a. Records of Access Rights. ProfitWell maintains a record of security privileges of individuals having access to customer data.

b. Access Authorization. ProfitWell maintains and updates a record of personnel authorized to access systems that contain customer data, deactivates authentication credentials of employees or contract workers immediately upon the termination of their employment or services, and identifies those personnel who may grant, alter, or cancel authorized access to data and resources.

c. Least Privilege. Technical support personnel are only permitted to have access to customer data when needed for the performance of their job function. ProfitWell restricts access to customer data to only those individuals who require such access to perform their job function.

d. Integrity and Confidentiality. ProfitWell instructs its personnel to disable administrative sessions when leaving ProfitWell's premises or when computers are unattended and stores passwords in a way that makes them unintelligible while they are in force.

e. Authentication. ProfitWell uses commercially reasonable practices to identify and authenticate users who attempt to access information systems. Where authentication mechanisms are based on passwords, we require that the passwords are renewed regularly and be at least eight characters long. ProfitWell ensures that de-activated or expired identifiers are not granted to other individuals. ProfitWell maintains commercially reasonable procedures to deactivate passwords that have been corrupted or inadvertently disclosed or pursuant to a number of failed login attempts. ProfitWell uses commercially reasonable password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

f. Network Design. ProfitWell has controls to avoid individuals assuming access rights they have not been assigned to gain access to customer data they are not authorized to access.

3.12 Network Security. ProfitWell's information systems have security controls designed to detect and mitigate attacks by using logs and alerting. ProfitWell implements endpoint protection on its hosting environments, including antivirus; which are continuously updated with critical patches or security releases in accordance with ProfitWell's server change control procedures.

3.13 Information Security Incident Management. ProfitWell maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.ProfitWell tracks disclosures of customer data, including what data has been disclosed, to whom, and at what time.

3.14 Business Continuity Management. ProfitWell employs redundant storage and its procedures for recovering data are designed to attempt to reconstruct customer data in its original state from before the time it was lost or destroyed.

PRIVACY

EU-U.S. AND SWISS-U.S. PRIVACY SHIELD FRAMEWORKS

200OK, LLC complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. 200OK, LLC has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/.

ProfitWell is responsible for the processing of personal data it receives, under each Privacy Shield Framework, and subsequently transfers to a third party acting as an agent on its behalf. ProfitWell complies with the Privacy Shield Principles for all onward transfers of personal data from the EU and Switzerland, including the onward transfer liability provisions.

With respect to personal data received or transferred pursuant to the Privacy Shield Frameworks, ProfitWell is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, ProfitWell may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

In compliance with the Privacy Shield Principles, 200OK, LLC commits to resolve complaints about our collection or use of your personal information. EU and Swiss individuals with inquiries or complaints regarding our Privacy Shield policy should first contact 200OK, LLC at:

Patrick Campbell, CEO, patrick@profitwell.com.

200OK, LLC has further committed to refer unresolved Privacy Shield complaints to an alternative dispute resolution provider located in the United States. If you do not receive timely acknowledgment of your complaint from us, or if we have not addressed your complaint to your satisfaction, you may visit https://www.jamsadr.com/eu-us-privacy-shield for more information or to file a complaint (free of charge).

To facilitate fast and convenient resolution of complaints, you agree to participate in online dispute resolution through JAMS Online Mediation (Endispute).

Under certain conditions, Privacy Shield provides the right to invoke binding arbitration when other dispute resolution procedures have not provided resolution. This is described in Annex I to the Privacy Shield.

COLLECTION:

We may collect the following personal information from you:
Contact Information, such as name, email address, mailing address, or phone number;
Demographic information, such as age, education, gender, interests and zip code;
Billing Information, such as credit card number and billing address;
Unique Identifiers, such as username, account number or password;
Geo location based on IP address;
Information about your business, such as company name, company size, business type.
We may also collect, from you, personal information about your contacts such as Name and email address where we can send receipts of your purchases. When you provide us with personal information about your contacts we will only use this information for the specific reason for which it is provided. If you believe that one of your contacts has provided us with your personal information and you would like to request that it be removed from our database, please contact us at the contact information below.

As is true of most websites, we gather certain information automatically. This information may include Internet protocol (IP) addresses, browser type, Internet service provider (ISP), referring/exit pages, the files viewed on our site (e.g., HTML pages, graphics, etc.), operating system, date/time stamp, and/or clickstream data to analyze trends in the aggregate and administer the site.

ProfitWell and its partners use cookies or similar technologies to analyze trends, administer the website, track users' movements around the website, and to gather demographic information about our user base as a whole. You can control the use of cookies at the individual browser level, but if you choose to disable cookies, it may limit your use of certain features or functions on our website or service.

USE:

The personal information as indicated being collected above is used for billing, identification, authentication, service improvement, research, and contact.

INFORMATION SHARING:

1. With Third Parties:

    We may share your information with third-party business partners, for instance, for the purpose of enhancing our products and services. If you do not want us to share your personal information with these companies, contact us at the contact information below.

2. With Service Providers:

We may share your information with third parties who provide services on our behalf to help with our business activities. These companies are authorized to use your personal information only as necessary to provide these services to us, to which these services may include:

- Payment processing
- Providing customer service
- Sending marketing communications
- Conducting research and analysis
- Providing cloud computing infrastructure

3. With Public Authorities or Law Enforcement:

In certain situations, ProfitWell may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. We may also disclose your personal information as required by law, such as to comply with a subpoena or other legal process, when we believe in good faith that disclosure is necessary to protect our rights, when we believe there is a violation to our Terms of Service (see ProfitWell Terms of Service), protect your safety or the safety of others, investigate fraud, or respond to a government request. If ProfitWell is involved in a merger, acquisition, or sale of all or a portion of its assets, you will be notified via email and/or a prominent notice on our website, of any change in ownership, uses of your personal information, and choices you may have regarding your personal information. We do not sell, rent or share personal information with third parties without your prior consent.

ACCESS

Upon request ProfitWell will provide you with information about whether we hold any of your personal information. You may access, correct, or request deletion of your personal information by logging into your account or by contacting us at the contact information below. We will respond to your request within a reasonable timeframe. In certain circumstances we may be required by law to retain your personal information, or may need to retain your personal information in order to continue providing a service.

200OK, LLC acknowledges that you have the right to access your personal information. ProfitWell has no direct relationship with the individuals whose personal data it processes. An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data should direct their query to the 200OK, LLC's Client (the data controller). If requested to remove data we will respond within a reasonable timeframe. In certain circumstances we may be required by law to retain your personal information, or may need to retain your personal information in order to continue providing a service.