TECHNOLOGY

1. What are the technologies used?

BuyingStation uses PSR coding language which is an open-source standardised coding style and development practise for PHP Projects. MySQL is used for database management and is managed by AWS. We use tools such as SonarQube and Duster to check the code quality in conjunction with our standard quality assurance process. BuyingStation uses separate hosting strategies for Laravel and Nuxt.js, utilising different server environments to optimise performance and scalability which consists of Laravel Hosting (Apache Server and MySQL Database) and Nuxt.js Hosting (AWS S3 and CloudFront).

2. Where is our platform hosted and what backup and security is in place?

BuyingStation is hosted on AWS which is backed up daily in the UK. AWS is a cloud computing platform offering scalable and flexible hosting solutions.

Data is transferred to AWS servers through encrypted channels (SSL) to ensure secure transmission from client devices to the platform.

AWS is considered highly secure, with a shared responsibility model:

- AWS manages the security of the cloud (hardware, software, networking and facilities).
- Customers manage security in the cloud (data, applications, identity, etc.)

BUYING STATION

AWS security features include:

- Encryption at rest and in transit.
- Identity and Access Management (IAM).
- Firewalls and DDoS protection.
- Logging and monitoring tools.

AWS complies with numerous global standards, including:

- ISO 27001, 27017, 27018 – Information security and cloud-specific controls.
- SOC 1, SOC 2, SOC 3 – System and organisation controls.
- GDPR – European data protection regulation.
- PCI DSS – Payment card industry standards
- HIPAA – U.S. healthcare data protection
- FedRAMP – U.S. government cloud security

Leading organisations including Netflix, Spotify and NASA also trust AWS for platform hosting and security.

Where is data collection and storage held?

- **Data Collection:** Data is directly uploaded by the client through a secure user interface on the BuyingStation platform.

- **Data Storage:** All client data is securely stored in the AWS cloud servers located within the UK. Detailed Privacy policy is available at the link provided below.

SECURITY

SECURITY MEASURES

1. **How are updates and patches delivered and are they automatic?**

   Updates are deployed automatically to the web application. No action is needed from users.

2. **What is the frequency of updates (scheduled or on-demand)?**

   - Regular updates are scheduled (e.g. weekly or every 15 days)
   - Urgent fixes, like security patches, are applied instantly as needed.

3. **How are customers notified of updates or maintenance windows?**

   - Notifications are sent via email.
   - Advance notice is provided for planned maintenance or downtime.

4. **Are detailed release notes provided for each update?**

   Yes, release notes are shared for every update, for new features, improvements and fixes.

VULNERABILITY MANAGEMENT

5. How quickly are critical vulnerabilities patched after identification?

Critical vulnerabilities are typically patched within 24–72 hours of identification, depending on complexity and testing requirements.

6. Are zero-day vulnerabilities addressed with emergency fixes?

Yes, zero-day vulnerabilities are prioritised and addressed with emergency patches to minimise risk.

7. Does BuyingStation monitor vulnerability databases (e.g. CVE, NVD)?

Yes, BuyingStation actively monitors trusted vulnerability databases like CVE and NVD, along with other industry sources, to stay ahead of potential threats.

8. Are vulnerabilities reported by customers or third parties acted upon promptly?

Absolutely. BuyingStation has a dedicated process to validate, prioritise and address reports from customers or third parties without delay.

SECURITY AND TESTING

9. What testing processes are in place before patches are released?

Patches go through rigorous testing and manual quality assurance reviews, to ensure reliability.

10. Are patches tested in a staging environment for compatibility?

Yes, all patches are tested in a testing and staging environment to identify and fix compatibility issues before deployment.

11. Do you conduct regular penetration tests and security scans?

Yes, we perform penetration testing, as well as perform regular security scans to identify vulnerabilities and ensure robust defences.

12. How are updates aligned with Microsoft 365 services to prevent disruptions?

BuyingStation does not currently have Microsoft 365 integrations. However, if required in the future, this will be addressed appropriately.

CUSTOMER IMPACT

13. Do updates or patches cause downtime and how is this communicated?

- Most updates are deployed with no downtime.
- For updates requiring downtime, customers are notified in advance via email.

14. Are rollback options available if a patch causes issues?

Yes, rollback mechanisms are in place to quickly restore the previous version if a patch causes problems.

15. Is customer action required post-update (e.g. re-authentication or validation)?

Generally, no action is required. If specific steps are needed, such as reauthentication or validations, clear instructions are provided in notifications.

MONITORING & REPORTING

16. **Does BuyingStation continuously monitor for threats and vulnerabilities?**

    Yes, threats and vulnerabilities are monitored using advanced tools and databases.

17. **Are vulnerability and patch reports available to customers?**

    Not at the moment.

COMPLIANCE

18. **Is the patching process aligned with standards like ISO 27001, SOC 2, or NIST?**

    BuyingStation has its own custom patching in place for managing information security and data protection. BuyingStation is proud to hold ISO 27001 certification.

19. **How does BuyingStation ensure compliance with regulations like GDPR or HIPAA?**

    BuyingStation adheres to GDPR and HIPAA by implementing strict data protection measures, conducting regular audits and ensuring patches address compliance-related vulnerabilities promptly.

INCIDENT AND THREAT RESPONSE

21. **How are customers notified of vulnerabilities that impact their data or services?**

    Customers are promptly notified via email.

22. What is the escalation process for critical vulnerabilities (e.g. Log4j-type incidents)?

For critical vulnerabilities, the escalation process includes:

- Issue Detection: The custom logging system tracks and flags critical vulnerabilities.
- Assessment: The security team quickly assesses the severity and the potential impact.
- Fix Development: A patch or fix is developed and tested immediately.
- Deployment: The fix is deployed as quickly as possible with minimal disruption.
- Customer Communication: Customers are notified of the issue and resolution status via email.

23. Do you leverage threat intelligence to address emerging risks?

Yes, we actively leverage threat intelligence feeds and security reports to identify and address emerging risks, ensuring proactive protection against new threats.

4. Disaster recovery / business continuity plan

1. Detection and initial assessment of the data breach

- BuyingStation identifies a potential data breach through monitoring, system alerts or reports from employees/third parties.
- BuyingStation to conduct an immediate initial assessment to determine the nature and extent of the breach. This includes identifying the type of data affected, the number of clients impacted and the root cause of the breach.
- The level of risk to the rights and freedoms of individuals will also be assessed. If the breach is likely to result in significant harm (e.g. identity theft, financial loss), BuyingStation will proceed to notify all relevant stakeholders.
- BuyingStation will start filling out the following Data Breach Incident Report Form.

2. Notification to the Data Protection Authority (DPA)

- Within 72 hours of becoming aware of the breach, BuyingStation will notify the relevant Data Protection Authority (DPA). This notification will include the nature of the breach (type of data and categories of people affected), the likely consequences of the breach and measures taken/proposed to mitigate the breach.
- If the notification to the DPA is beyond 72 hours, reasons for this delay will be provided by BuyingStation.

3. Client notification of the data breach

BuyingStation will identify ALL clients whose data has been compromised as part of the breach, ensuring full accuracy in the identification process. A clear and concise data breach notification will be provided to each affected client, which includes:

- What happened – a factual description of the breach, including when it was detected and the nature of the breach (e.g. unauthorised access, data theft).
- What information was compromised – details of the categories of personal data affected (e.g. company records, financial details, contact information).
- Consequences – an explanation of the potential risks or impact on the client (e.g. identity theft, potential misuse of personal data)
- Measures taken – describes the immediate actions taken by BuyingStation to address the breach (e.g. securing systems, changing passwords, patching vulnerabilities).
- How BuyingStation are managing the situation – outlines the efforts to contain the breach and prevent any future reoccurrence, including collaborating with relevant teams to ensure security.
- Advice to the client – provides guidance on what the client should do to protect themselves (e.g. monitor all accounts, change all passwords, being alert to any suspicious activity).
- Point of contact – includes contact information for clients to ask questions, request further details or seek support (e.g. IT Support team or contact details for our DPO).

Client notification will be sent without any delay, ideally immediately after the internal assessment has been carried out and the risk has been confirmed.

4. Internal response and containment measures

- BuyingStation will implement immediate measures to contain the breach, such as revoking unauthorised access, isolating affected accounts and conducting a security audit of the platform.
- BuyingStation will establish a comprehensive plan to address the vulnerabilities that caused the breach. This includes strengthening BuyingStation's security, updating policies and improving staff training.

5. Mitigating further damage

- BuyingStation will offer support to affected clients, such as credit monitoring services, access to an IT helpline or cybersecurity advice via Apex Analytix. Ongoing updates to be provided to the client, advising them on progress.
- BuyingStation also encourages all clients to use the Multi-Factor Authentication functionality.

6. Documentation and reporting

- BuyingStation documents the breach in high detail, including how it was detected, the steps taken to mitigate it and the communications sent to both the DPA and affected clients. This ensures compliance with the GDPR.
- A final report will be produced summarising the overall cause of the breach, how it was managed and any lessons learned. This report can be shared internally and used for audits or any further investigations.

7. Review and improvement

- BuyingStation will conduct a thorough review of the breach incident to assess the effectiveness of the response and identify any areas for improvement.
- BuyingStation will revise the company's GDPR policy, security protocols and staff training to prevent future incidents.