Boardingware

Navigating GDPR Compliance

TECHNICAL WHITEPAPER

LAST UPDATED: May 1, 2018 11:50 AM

Contents

Our Commitment to the GDPR

Boardingware provides a software service that enables schools to keep track of their students online. As a processor of sensitive staff and student information, we understand the importance of data security and privacy and take our role very seriously. We pride ourselves on being a trusted partner to our schools and are fully-committed to delivering a secure, enterprise service that's GDPR compliant.

In May 2018, a new EU General Data Protection Regulation (GDPR) will come into force which implements a number of obligations for ANY organisation who handles personal data relating to people in the EU.

To comply with GDPR, schools may need to overhaul and update a number of internal processes and systems. They will also need to assess the risk from third-party vendors (aka data processors) used to process personal data.

Article 28 of GDPR states that "The controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject,"

This means that your school may also be liable if one of your third party services are breached for failing to adhere to GDPR requirements. To ensure this doesn't happen, schools will need to assess all Third-Party services they use to confirm that they are also GDPR compliant.

This can be a time-consuming process for schools that use many different third-party processors. So to help you fulfill your due diligence, we created this whitepaper to explain how Boardingware meets GDPR compliance and provide answers to the questions commonly found in GDPR vendor assessment templates.

I hope you find the information in this whitepaper useful and if you require any further information regarding Boardingware's GDPR compliance, please do not hesitate to contacts us at privacy@boardingware.com

Our Role as a Controller and Processor

Boardingware acts as both a data processor and data controller under the GDPR.

Boardingware as a data processor

When customers use Boardingware to process personal data - for example, when schools invite students to create a Boardingware account - Boardingware acts as the data processor. Customers can use the controls available in the Boardingware service, including access and security configuration controls, for the handling of personal data.

Boardingware as a data controller

When Boardingware collects personal data and determines the purposes and means of processing that personal data - for example, when Boardingware stores staff account information for account registration, administration, service access or contact information for the Boardingware account to provide assistance through customer support activities - it acts as a data controller.

Governance

One of the underlying principles of the GDPR is to ensure that organizations place data governance at the heart of what they do.

To comply with GDPR and ensure that we meet the expectations of our customers, we have assigned a designated Data Protection Officer and defined clear roles and responsibilities for our executive team to raise awareness of privacy issues and embed privacy compliance into the mind-set of Boardingware employees, so that we can be proactive with data protection, not reactive.

Lawfulness, Fairness and Transparency

One of the core GDPR principles requires organizations to ensure that personal data is "processed lawfully, fairly and in a transparent manner in relation to the data subject". Boardingware has implemented the following policies to ensure we comply with this requirement:

Conditions of Consent

To ensure that the processing of personal data is "Lawful", Boardingware has controls in place to ensure a lawful basis for processing is identified upon collection. When processing is based on consent from the data subject, Boardingware will adhere to the following conditions:

- Consent is given from an individuals own free will and without force.
- Data subject is clearly informed, in plain language, what exactly is being asked of them and how they can opt-in or out.
- Positive action must be used to indicate consent (ie. the person must submit a form or tick a box to give indication of their consent)

Purpose limitation

To ensure that the processing of personal data is "fair", Boardingware has implemented controls to ensure that the purpose for processing is documented upon collection to ensure that it is only processed for its intended purpose(s).

Privacy Policy

To ensure that the processing of personal data is "transparent", Boardingware will inform data subjects about what to expect from the processing of their personal data. This information will be communicated through our privacy policy which will be made publicly available; concise, intelligible and written in clear and plain language; and provided free of charge. Click here to view our updated privacy policy.

Individual Rights

Data subjects are given more extensive rights under the GDPR. At Boardingware we have implemented the following procedures to enable our customers and end-users to exercise their rights at any time:

Providing right to access and rectify information

Individuals may review, correct, and/or update their information with the settings and tools provided in their Boardingware account or by making a request via email to privacy@boardingware.com

Complying with request to erase information

If a request for erasure has been received, Boardingware will first verify the identity of the requester before erasing their data, including back up copies.

Complying with request to provide copy of information

If requested, Boardingware can export customers data in a machine readable format such as CSV or SQL and send it to the requester in an encrypted format via email. Free of charge.

Providing right to restrict or completely withdraw consent to processing

Individuals are explicitly informed of their right to opt-out and withdraw consent for Boardingware to control their data.

Privacy by Design and by Default

Privacy by design is an approach that promotes privacy and data protection compliance from the start of the development process. Under the GDPR, organizations now have a general obligation to implement technical and organisational measures to demonstrate a consideration for 'Privacy by Design'.

Secure Development Policy

At Boardingware, we have implemented a '*Secure Development Policy*' that establishes clear controls to ensure that information security is taken into account throughout the entire development lifecycle. The principles in this policy apply to all types of development within Boardingware, including the creation of marketing systems, customer support systems, internal operational systems, as well as the development of cloud web and mobile applications. Our secure development policy implements the following controls:

Planning and Analysis

Security Analysis and Data Privacy Impact Assessments (DPIAs) are conducted during the planning and analysis phase. This helps to identify any potential risks, identify controls to mitigate/eliminate risks and ensure that any requirements are fulfilled throughout development.

Design and Implementation

Secure development methodologies, version control, quality assurance, secure development environments, restrictions to software packages and rules for outsourcing development are implemented to ensure the development of projects are effective and secure.

Testing and Deployment

Strict rules for testing methods and test data are enforced to ensure customer data is not affected during the testing phase. Deployment procedures are designed to release new features within little to no disruption to existing services and to ensure rollback capabilities are available in the case that a deployment goes unexpectedly wrong.

Monitoring and Maintenance

Considerations for monitoring the effectiveness of projects throughout all the development phases are taken into account. Continued maintenance of new projects are taken into account including the consideration of future updates and ongoing overheads to ensure the continued quality and reliability of releases.

Privacy by Default means that when a system or service includes choices for the individual on how much personal data he/she shares with others, the default settings should be the most privacy friendly ones. To support this, article 25 of the GDPR states that the controller "shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed." To ensure that Boardingware and their customers comply with this requirement, the following '*Data Access Controls*' have been implemented:

Access Controls for Boardingware customers:

Authentication

Unique identification and authentication credentials are required to secure access to customers Boardingware accounts

User Access Permissions

Application settings provide authorized users with granular controls to manage access permissions for different user types. This includes:

- System permissions to control which users can edit, delete or view information.
- Access permissions to control which users can access student houses.
- Feature permissions to control which features users have access to.

User Management

Authorized users are provided with user management capabilities to remove users, suspend users, reset passwords and view recent activity.

Auditing Capabilities

Authorized users are provided with auditing capabilities to record and review who accesses, edits, deletes and exports personal information within Boardingware.

Access controls for Boardingware employees:

Internal policies and systems have been implemented to assign appropriate access controls to company assets based on Boardingware's business and security requirements. The following controls are intended to enforce that access to information is managed on a "need to know basis", employees always protect their access and information is accessed securely.

Access Management

Access profiles are created and defined by business functions to determine which assets an employee is allowed to access by default. By default, this is limited to a "need to know" and "need to use" basis. There is are request processes that must be followed if an employee needs to gain special access to assets that are not assigned to their role.

Secure Access

Controls are in place to ensure employees only access information assets via networks with WPA2 and enable SSL protection when transmitting sensitive information. Highly sensitive information is restricted to authorised IP addresses.

User Management

Boardingware personnel are assigned unique IDs which must be used for registering to business assets. Each account uses this ID which enables Boardingware to track use of assets and hold employees responsible for their correct use.

Password Policy

A password policy is in place to ensure employees set strong passwords and manage their protection effectively to protect against generative password attacks. Rules for sharing and inputting passwords are enforced to avoid unauthorised disclosure.

Data Security

In order to "future proof" data privacy, the GDPR requires organizations to regularly review and implement "State of The Art" information security solutions and processes to protect personal data in the best possible way.

To meet these data security requirements, Boardingware has implemented a full Information Security Management System according to the ***ISO 27001, 27017 and 27018 standards*** (due to be certified in June 2018). This helps to demonstrate that Boardingware has implemented sufficient technical, administrative and physical safeguards required to protect the confidentiality, integrity and availability of personal information.

As part of our Information Security System, we have implemented the following controls to provide state-of-the-art data security to our customers:

Cryptographic Controls

Cryptographic controls are used throughout Boardingware's operational systems and products to ensure protection of critical business information and compliance with any legal, regulatory or contractual obligations. This includes the encryption of confidential or sensitive information, encryption of networks, encryption of work devices, and detailed encryption specifications to be implemented throughout the development of Boardingware's cloud and mobile products, such as - encryption at rest and in transit.

Data Recovery Processes

Boardingware's cloud infrastructure and backup protocols mean that in the event of a physical or technical incident, we can restore the availability and access to personal data in a timely manner

Data Retention Policy

Personal information is only retained for the time defined as needed for the achievement of its intended purpose. If personal information is no longer required to fulfil its intended purpose, it will be systematically destroyed, erased or anonymized.

Performance Review

All processes and protocols are regularly tested, assessed and evaluated to ensure our technical and organisational measures are effective for the security of processing.

For more information about our Information Management System and Cloud Security Protocols, refer to the supporting whitepapers below:

- Cloud Security Whitepaper
- Information Security Whitepaper

Data Breach Readiness and Response

As part of our Information Management System, we have an implemented an *Incident Management Procedure* to ensure the consistent and effective approach to the management of information security incidents, including the responsibility of reporting security events and weaknesses.

In the case of a personal data breach that is likely to result in high risk to the rights and freedoms of the data subject, Boardingware will notify the affected persons no later than 72 hours after becoming aware of the incident. Boardingware may also notify the supervisory authority if required by the GDPR.

Data Transfers

Boardingware SaaS systems are contained in highly available AWS data centers in multiple regions, including the European Union (Ireland). This means that personal information doesn't have to be transferred to a third country and customers can benefit from storing their personal information within their own geographical region.

In addition to the European Union, Boardingware also has storage availability zones in North America (Virginia) and Australia (Sydney). Within each region are multiple availability zones which gives Boardingware the ability to move customer data and traffic away from any affected availability zones in the event of a failure. Availability zones can also be used for load balancing so spikes of traffic will reduce the chance of related server crashes.

The location chosen to store personal data is decided by the customer and included in the service agreements.

Supplier Agreements

Boardingware may use third-party cloud services to process personal information for business operations. This means that data may be transferred to countries outside of the European Union. To ensure that personal data is processed in accordance or with similar standards to the GDPR, Boardingware is responsible for acquiring appropriate supplier agreements as stated in our '*Supplier Security Policy.*'

Binding corporate rules or similar mechanisms are implemented with all our third-party services that interact with personal information to ensure that their security levels meet Boardingware's security requirements, and that security measures will not be reduced by unilateral decisions made by suppliers.

Conclusion

We take security seriously at Boardingware, because every person and team using our service expects their data to be secure and confidential. Safeguarding this data is a critical responsibility we have to our customers, and we work hard to maintain that trust.

If you have any further questions about our processes to comply with GDPR, please contact us at security@boardingware.com.

Boardingware