Data Protection Impact Assessment

13 April 2022

This document acts as a Data Protection Impact Assessment for the MyHallWizard system which is provided as Software as a Service. It covers both MyHallWizard user data, for which HallWizard Limited is the data controller, and customer data for each venue, for which the Account Holder of the venue is the controller and HallWizard Limited is a processor. As such, information in this document may be made available to Account Holders on request.

Submitting controller details

Name of controller	The data controller for MyHallWizard users is HallWizard Limited. The data controller for venue customers is the Account Holder. HallWizard Limited is a processor.
Subject/title of DPO	A DPO does not need to be appointed by HallWizard as: • HallWizard is not a public authority or body • HallWizard's core activities do not require regular and systematic monitoring of individuals on a large scale • HallWizard's core activities do not involve processing on a large scale 'special categories' of personal data, or 'criminal convictions or offences data'
Name of controller contact (delete as appropriate)	HallWizard's controller contact is Nicholas Savill, Director

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
The MyHallWizard system manages the booking, invoicing and payment tracking of room bookings in venues such as church and village halls. The system records names and contact details of its users. Users of the system can record names and contact details of their customers. For this data, HallWizard is a processor. A DPIA has been prepared because HallWizard Limited may be required to assist Account Holders (data controllers) in producing their own DPIAs.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

MyHallWizard Users

MyHallWizard user information will be collected directly from the user, who completes an online form. Data will be used for account management, customer support, and marketing.

User information is accessible only by the user themselves and by HallWizard support staff.

User information is shared with third parties for the purposes of HallWizard administration. This includes HubSpot (customer support and CRM) and Paddle.com (Merchant of Record for all orders).

Venue Customers

Venue customer information is input into the MyHallWizard system by users. Data is used by the venue for bookings, invoicing, and payment tracking. Customer information may also be included in reports generated by the venue.

Customer information is accessible only by MyHallWizard users who have been authorized by the venue's Account Holder, and by HallWizard support staff while providing support to a venue's user.

Venue customer information is not shared with any third party or used by HallWizard for any other purpose.

Web Analytics

We use Google Analytics to record how our website and MyHallWizard are used. This may identify demographics of the user, but does not record any personally identifiable information.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
Data recorded includes name, address, phone number, email address, billing information, contact and correspondence history, and an audit trail of any data changes performed by the user. No special category, sensitive or criminal offence data is recorded. Data for users will be retained while they are active users of the system. After cancellation of an account, user information will be retained for 90 days. MyHallWizard can be accessed globally, though we have geographical restrictions to prevent access to the system from countries where we are not allowed to sell by law, and from any countries we consider to pose a significant security risk. Personal data is stored in an EU-based data centre in the Republic of Ireland, but data access is currently from the UK. Standard Contractual Clauses are used to permit the movement of EU data to the UK. No detailed review of non-EU data protection requirements has been performed, though we believe the data protection proposed is lawful for the USA.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
Users have full control over their personal details on the system, including name, address, phone number and email address. Venue customers do not currently have direct control over data within the system, and need to request any amendments directly with the venue. All data recorded is reasonable and proportionate to the business context, and data subjects would consider it reasonable that HallWizard uses its data in this way. MyHallWizard is a B2B system, and so is not targeted at children or vulnerable groups. There are no known concerns over this type of processing, no known security flaws, and the processing is not novel. The technology of the MyHallWizard system is an implementation of the Laravel framework, including various associated packages to manage security and billing. The system is hosted on AWS using Laravel Forge. A web application firewall provides protection against DDoS attacks and malicious requests and attack patterns. Daily vulnerability checks are performed on the software using Snyk, and vulnerabilities are resolved as quickly as possible. The MyHallWizard system uses privacy by design to ensure that venues do not have access to each others' data, that users of the system are only able to view data they are authorized to see. A geography-based firewall prevents access to the website and application from certain countries. In particular, this has been configured to exclude access from countries known to be hotbeds of system hacking such as Russia and China. It also excludes access from countries from which it is not legal for HallWizard to do business. Account Holder payment card details are not stored in the MyHallWizard system, but within Paddle.com which has a very high level of security. HallWizard staff do not have access to card data.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?
The system has two aims: 1. To allow venues to manage their bookings, customer databases, invoicing and payment tracking 2. To allow HallWizard Limited to provide a service to venues

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
HallWizard Limited takes professional advice directly or through research on the Internet on an ongoing basis to ensure compliance with all legal and data protection requirements.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
The lawful basis for processing is legitimate business interests. The minimum data necessary to achieve HallWizard's and the venues' needs is recorded. Data quality of user information will be achieved by annual emails to confirm all details are correct. A Privacy Policy is available on all pages of HallWizard's website and application providing detailed information on the data collected and how it is processed. The Privacy explains the rights of data subjects and how they can exercise them. Our vision is to provide tools to users and venues to allow them to self-service Subject Access Requests in both human and machine-readable formats. Until this software has been developed, SARs need to be raised via HallWizard Support, who will prepare the required report manually. Customers' rights to be forgotten, to restrict processing or to object to processing can be fulfilled by deleting the relevant customer record in MyHallWizard.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Unauthorised access or modification to the application data	Possible	Minimal	Low
Inadequate protections (i.e. failures of privacy by design) within the system, allowing users to see personal data they are not authorized to see	Possible	Minimal	Low
Stolen credentials	Remote	Severe	Medium
Stolen payment details	Remote	Severe	Medium
Vulnerabilities in the code and its libraries	Remote	Minimal	Low

Data loss	Remote	Minimal	Low

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no
Unauthorised access or modification to the application data	Full application and technology security is applied Strong IAM policies Secrets are not accessible from public domains Although the database is publicly accessible it is protected by long, very strong password. We plan to remove public accessibility in the future. AWS account and Laravel Forge account require Multi-Factor Authentication.	Reduced	Low	
Inadequate protections (i.e. failures of privacy by design) within the system, allowing users to see personal data they are not authorized to see	It is mandatory to test privacy by design in automated tests of all functional areas of the system.	Reduced	Low	
Stolen credentials	Insurance	Accepted	Medium	

Stolen payment details	This is mitigated by only storing payment details in Paddle.com. Risk transfer via Insurance	Accepted	Medium	
Vulnerabilities in the code and its libraries	Daily scans using Snyk and resolution as soon as possible, dependent on the criticality of the vulnerability and the availability of a resolution.	Reduced	Low	
Data loss	Production database is flagged to prevent deletion The database user does not have privileges to drop tables. All user tables used for operational data are set to soft delete, ensuring that code cannot accidentally delete data. Data is hard deleted after 30 days. All data changes to operational data tables and venue configuration are recorded in the audit table, enabling changes to be tracked and reversed. All data is replicated to backup on a real-time basis and retained for 3 days. The database can be restored to any point within the 3 day retention window. Daily backups of data are performed with backups being retained for 30 days.	Reduced	Low	

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion

	Nicholas Savill Director 13 April 2022	
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA