Redburn data security measures for vendors and partners

Redburn Innovations Ltd,
2nd Floor, 2 Cornhill, Bury St Edmunds,
Suffolk, IP33 1BE, United Kingdom.
Company Number: 8846588

Redburn Innovations Data Security Measures for Vendors, Partners and Suppliers

Purpose

The purpose of this document is to enable the assessment of the organisational and technical approach to data security and records management within Redburn Innovations Ltd to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. It is intended to provide additional information and detail for our Vendors and Partners, and contributes towards our General Data Protection Regulation (GDPR) compliance plan.

What is Personal Information?

General Data Protection Regulation, Article 4, Definitions

> (1) 'personal data' means 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;

Scope

This personal data includes

1. Customer personal data on our live systems and servers: consent to our Privacy Policy has been received for all confirmed bookings.
2. Diagnostic log files that are a routine record of events on our systems: consent to our Privacy Policy has been received for all confirmed bookings.

3. Back up data that is copied onto HDD (or any backup media). User data is stored on HDD on our servers. Periodically, backup copies of this data are saved onto HDD (or other media). This is useful in case of a system failure. This Allows us to go back into the past if necessary to help with enquiers of potential deleted data. I.e. If a customer says they booked on a date 7 months ago, we restore this and check the data to see what has happened. This is because we delete uncompleted bookings after 1 month. Consent to our Privacy Policy has been received for all confirmed bookings.
4. Vendor data on our systems, computers, and in googledocs. Consent to retain this data has been received via the Vendor Agreement.
5. Customer or Vendor emails stored on our mail server.
6. Customer or Vendor information retained on physical form.
7. Employee Data.

Record Types

This policy addresses

1. Customer, vendor, or internally-generated electronic data
2. Electronic diagnostics data generated by our systems in various formats (.txt, .tar, .zip, etc)
3. Hard copy data

The retention policy does not include

data records not controlled by SpeedyBooker

Roles

The retention of data and determination of useful retention of system logs is determined by system administrators and our CTO, who is our Data Protection Officer, and one other individual for continuity reasons when the CTO is out of the office.

System administrators are responsible for the execution of retention and adherence to the schedule.

Our Privacy Policy

Our Privacy Policy outlines the data we collect from customers, the uses of this data, who we share it with, and where we store it.

Controlling and Sharing Customer Data with Vendors

Our policies with Vendors concerning protecting customer data are set out in clause 7 of our agreement with Vendors entitled “Data Protection”.

Data Retention Policy

1. Customer personal data will retained by SpeedyBooker indefinitely until such time that the customer requests it to be removed. This is because any customer may wish to login to our websites at any time to make another booking, update their personal data, or access their historic booking data. Customer personal data will not be visible after 7 years, instead marked “Hidden”. This is to allow Vendors to monitor and track repeat customers, such as Hotel guests that have returned for many years and may be eligible for loyalty rewards, or university students that are studying long courses such as medicine (6 years) and where the vendor needs to check the booking/room history.
2. Diagnostic logs relating to customer and vendor activity will be automatically and permanently deleted after 2 years as it is not necessary to retain this data longer than that.

3. Back up data is retained for up to one year, even if the customer has requested deletion of their personal data.
    a. This data is retained for business continuity and diagnostic purposes only. For example, if data is lost from the live system, we may need to restore historic booking data to fulfil our obligations to provide Vendors with customer booking details.
    b. In this case, during the restoration process, any personal data that has been deleted from our live systems will automatically not be restored. Therefore, in the example above, any request to delete personal data will take priority over a Vendor's requirement to know the personal data of future customer arrivals, and the customer personal data will show as "Details deleted".
    c. In addition, within the Back up, all personal data is encrypted and can only be decrypted by System Administrators.
4. Vendor data will be retained for an unlimited period unless the vendor requests their data is deleted, in which case it will be deleted within a maximum of 30 days.
5. Emails may be retained for an unlimited period unless the sender requests their emails are deleted, in which case it will be deleted within a maximum of 30 days.
6. Information in physical form will be shredded within 1 year.

Questions and Answers

Purpose of the application	*Accommodation, event and ticket booking website and associated admin/property management system*
Where is the application accessible from?	*Online through the Internet*
Does the application store or collect sensitive personal data?	*No*
Does the application store or collect personal data?	*Yes*
What personal data does the application store or collect?	*Customer title, name, address, age bracket, telephone, email, car registration numbers, and passport/ID numbers, credit/debit card details.* *Vendor users: name, address, telephone, email.*
Does the application store or collect identity data?	*Yes*
What identity data is stored or collected?	*Customers: username, password, booking reference numbers* *Vendors: username, password.*
Data Sources, Storage and Access	
a. Where does the data come from?	*Customers: entered by the user on secure pages on our websites, including account creation or booking completion pages* *Vendors: entered by the user or our employees on secure sign up pages on our website or user profile creation on our admin system.*
b. Where is the data stored?	*Customer card data is stored by Opayo/ Acapture and is protected and secure.*

	Customer email addresses are stored on our the servers of Campaign Monitor, our email campaign partner, and are protected and secure. *Customer and Vendor personal and identity data is stored in our database, which is in turn stored on our servers which sit in a secure and professionally protected data centre owned and operated by Iomart Group Plc. These servers are protected by Microsoft Security Essentials anti-virus software. This software is updated automatically.*
c. Who has access to the application?	*Each employee and contractor of SpeedyBooker has varying access levels to personal and identity data, on a case by case basis depending on their business requirements according to the nature of their role.* *The database is locked down to specific IP addresses including that of our office, preventing access to anyone using a different IP address.*
d. Is there a data retention policy for this application?	*Yes*
(i) What is the policy?	*See above*
(ii) Does the application have a delete or archive[1] capability?	*Yes*
(iii) Have records ever been deleted?	*Yes*
(iv) What records have been deleted and when?	*Users have been deleted from our database when requested.*
e. Is the data regularly backed up?	*Yes*
(i) Where is the data backed up?	*Daily to disk*
f. Data Protection by Design	
(i) Data is MINIMISED – adequate, relevant and limited to what is necessary	*Green* *We only take the information we need to complete a booking and nothing else.*
(ii) Personal data are held encrypted, anonymised or pseudonymised	*Amber* *Customer First Name, Last Name, Address are not encrypted. Email address and login details are encrypted.*
(iii) Access to the data is based on role and least-privilege	*Green*

	Only a few team members can access to our database (which all have different privileges). Our admin system uses roles for each user, only three have full rights.
g. Does this application provide data to, or share data with 'downstream' applications, services, people or organisations?	*Yes*
(i) Please list or describe these applications, services, people or organisations	*Opayo (Payment gateway), First Data (card processing), AIB Merchant Services (card processing), Acapture B.V. (payment processing), Campaign Monitor (secure email platform).*
(ii) What sharing mechanisms are used?	*Web Service, API*
h. Can you give some indication of the number of records holding the different categories of data	*We currently store around 500,000 records holding personal or identity data.*
i. Do you have an internal Data Security Policy?	*Yes: all members of staff are required to sign to confirm they are familiar with our Data Security Policy every 12 months. This Policy includes practical measures for all staff to follow to protect all data.*
Consent	
a. Is consent required?	*Yes*
b. Comments around consent	*Before a customer completes a booking, their consent is required to a) our Terms and Conditions, b) our Privacy Policy, and c) whether they wish to opt in to "I would like to receive occasional email updates and promotions from you".*
Is there a Privacy Policy?	*Yes*
Is the application documented?	*Yes*
a. Is the documentation up-to-date and adequate?	*No, plans to improve this in the near future. Our code infrastructure has changed drastically over the past couple of months and as such our documentation needs to be updated.*
b. Is there technical/user/design documentation?	*Yes, detailed in our internal records.*
Is there a Data Processing Agreement (DPA)	*Yes, enclosed within Your vendor agreement.*
Other	
Does the application perform automated processing or make automatic decisions based on information given?	*No*
Does the application store data outside the EU?	*No*
Is the data held in the application deemed to be accurate?	*Yes*

Is there a storage limit for the application?	*No*
Does the application hold any financial data for individuals?	*No*
What format (plain text, audio, video, image) is data held in?	All uploaded vendor images are stored in .jpg/.jpeg format, no other formats are stored at this time.

[1] Archiving stores data that's no longer in day-to-day use but must still be retained.