GDPR Record of statement

For the: ***Invincible Leisure Ltd***
Last updated: *1st May 2018*
Approved by: *Finance and Operational Manager*

Introduction

Invincible Leisure Ltd, (‘’ we”) is a Limited organisation whose registered address is Venture House, The Tanneries, East Street, Titchfield, Hampshire, PO14 4AR. These address are securely locked and alarmed when not occupied.

Our primary purpose is a late night entertainment venue.

We have approximately 50 employed staff. .Invincible Leisure Ltd stores and processes some of its data remotely:

- ID Scan IDSCAN Policy
- Cloud-based platform providers Xero, Aviva and Fatsoma
- Management personal laptops
- Microsoft One Drive

All of the above are data processors to Invincible Leisure Ltd as data controller. We have GDPR compliant processor contracts in place with all of the above named parties. All processors undertake to keep the data within the EEA or are compliant and certified under the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks.

Invincible Leisure Ltd has sought legal and professional advice on matters of the GDPR from commercial law specialists at Warner Goodman LLP and the Information Commissioner’s Office. This document and the processes established in managing our data compliance has had oversight and guidance from their specialists and Voodoo Leisure’s Finance and Operations Team..

Policy Statement

1. Invincible Leisure intends to comply with GDPR or the same as subsequently enacted into UK domestic law at Brexit.

2. We will therefore:

    a. Only process as much personal data as is necessary for our administration and the services we supply.

    b. Only hold such data for so long as necessary for those purposes. In this connection we have decided that ten years following the last contact with an individual is usually an appropriate period to hold data covering the legal limitation period (six years) and a moderate margin. As in most cases this is only archived data, not sensitive, not dangerous and will not be used there seems little risk to data subjects.

c. Only process such data on grounds for lawful processing provided within GDPR Article 6.

d. Send or otherwise provide appropriate notices (GDPR Articles 13 and 14) to those whose personally identifiable information ("Personal Data") is processed by us including our employees, and individuals or individuals within partners who supply us with goods or services. We will also send such notices to individuals within organisations to whom generic marketing communications (eg newsletters) are sent.

e. CCTV and Bodyworn Policy.

f. Not engage in direct marketing to clients or prospects otherwise than in accordance with the relevant legislation and guidance from the ICO.

g. Scannet/IDScan - Admission Policy

h. Utilise appropriate organisational and technical measures to ensure that Personal Data processed by us is kept secure.

i. Where we use third party data processors we will choose them carefully with a view to their data security and compliance with GDPR and have GDPR compliant contracts with them.

j. Not transfer Personal Data (which includes giving third parties access to it within our IT system) to recipients located outside the European Economic Area and the UK without confirmation from our Data Protection Officer that such transfer is lawful.

k. Update this document from time to time so that it remains an accurate record of our data processing activities and policies.

3. The Finance Director is appointed as our Data Protection Officer.

4. Following legal advice we have concluded that GDPR is not intended to require us to treat employees of our current or prospective partners and suppliers whose contact details we are required to use for dealing with those organisations, nor individuals who contact us intending to engage in correspondence with us, as data subjects to whom we should send notices pursuant to Articles 13 and 14 merely because we hold and use those contact details in connection with our dealings with them or their employers, or keep copies of such communications, as the effect of such interpretation would be disproportionate.

5. We conclude that where we hold and process such personal data for the purposes of direct marketing to those individuals' employers we should, unless guidance from the ICO says otherwise, either:

a. obtain consent to that direct marketing from the individuals and send the notices required by Articles 13 and 14 to the individuals; or

b. be satisfied that we have a legitimate interest in holding that Personal Data and using it for that purpose.

6. Following legal advice we have concluded that when employee data is shared with our pension provider, insurance provider, payroll provider and HMRC, they are neither our processor nor joint controller of the data concerned as it is being provided for their own use as they see fit to provide a service to us and/or benefits to our employees and members. We will however, where possible, require contracts with them containing confidentiality obligations in respect of that data and other data that they create relating to our employees, members or customers in the context of the work they are doing.

Our processing

1. Customers and visitors

Personal data collected:	Image of individual, Postal Address as shown on ID, Full Name any other information shown on ID used to secure entry. Email address, Postal Address
Special categories of data collected:	None
Data origination:	Provided by individual
Storage location:	CCTV Control Units (Offline), Fatsoma, Lost property storage.
Identified data usage:	CCTV, Event ticket sales history, ID Scan entry system.
Third parties with access:	None
Retention period:	10 Years - CCTV and IDScan Data 31 days (unless alert applied)

2. Employees of suppliers, contractors and clients

Personal data collected:	Email Address, Full Name, Business Name, Postal Address, Role Title, Telephone, Signature and Bank Details
Special categories of data collected:	None
Data origination:	Provided by individual
Storage location:	Xero, Locked Filing Cabinet and One Drive.

Identified data usage:	Client invoices, supplier payments, marketing and communications, credit management and fraud prevention
Third parties with access:	Compass Accountants (Accountants), Xero - Accounting Software
Retention period:	10 Years

3. Employees of the Invincible Leisure Ltd

Personal data collected:	Email Address, Full Name, Telephone, Postal Address, Role Title, Date of Birth, NI Number, Bank Details, P45 / P46, Next of Kin Details, Disciplinary Record, Financial Bonding, Photographic ID, Right to work in UK, Reference Personal Details.
Data origination:	Provided by individual
Special categories of data collected:	Gender, Criminal Record and Personal Health Records
Storage location:	Locked Cabinet, HSBC, One Drive, Aviva and Xero
Identified data usage:	Employee Administration, Recruitment processes.
Third parties with access:	Compass Accountants, HSBC, HMRC, National Health Service
Retention period:	Recruitment records - 6 weeks after not being appointed to a role HR records - 10 years

4. Data Storage

Invincible Leisure stores and processes some of its data remotely:

- Microsoft who provide One-Drive Services
- Cloud-based platform providers Xero, Aviva and Fatsoma.

All of the above are data processors to Invincible Leisure as data controller. We have GDPR compliant processor contracts in place with all of the above named parties. All processors undertake to keep the data within the EEA or are compliant and certified under the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks.

5. Organisational and technical measures

We use the following organisational and technical measures to ensure the confidentiality of personal data:

a. Provisions that employees who process data are required to consider the use of lockable filing cabinets, secure storage for archived files and the use of a shredder or confidential waste bin for hard copies of paperwork, file notes, incoming and outgoing letter correspondence containing personal data.

b. For electronically held data employees who process data are required to consider using storage on the, work one drive or platforms approved by the Data Protection Officer, password protection on all files containing personal data, the use of the Voodoo Leisure's secure platforms for processing data, running up to date antivirus and malware systems,

installation of adequate firewalls, the secure destruction or disposal of IT equipment.

c. CCTV units are not networked and access to the systems are through password protected platforms. This data may only be accessed by those authorised by the Data Protection purposes or law enforcement agencies.

d. Email accounts are individually assigned and not shared with colleagues or third parties. Access to emails are only authorised for third parties for specific purposes by Senior Management Team members.

e. The data protection and information security handbook provides clear guidance on data sharing, data handling, security breach procedures and disposal of data.

f. We hold GDPR compliant contracts with all data processors.

g. All employees undertake training in data privacy law and cyber security before being given authorised access to process data held by Invincible Leisure Ltd

6. Consent

We do not engage in direct marketing to individuals except in their capacity as a member of our Company or as a conduit for our company.

Following consultation with the ICO and a review of the appropriate legislation we have concluded that as our customers have purchased through Fatsoma we do not need consent in communicating through digital means with our customers about our related products and services. We believe that as a customer there is a legitimate interest in receiving this information which is noted as a lawful reason for processing data in Recital 47. In all communications there is an opt-out and the customer will have received an article 13 or 14 notice prior to receiving any communications at all.

We will keep the proposed replacement of The Privacy and Electronic Communications (EC Directive) Regulations 2003 and guidance from the ICO under review.

We are aware that consent under GDPR must be freely given, specific, informed and unambiguous given by a statement or a clear affirmative action and that we have to keep a record of each consent obtained for as long as we are using it. We do not currently believe that any of our processing of Personal Data, except for the sending of the commercial marketing, requires data subject consent.

7. Legitimate Interests

Recital 47 of the GDPR reads: *"The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller."*

We rely on legitimate interest as justifying much of our processing of Personal Data as we have assessed that the majority of our processing activity would be in the reasonable expectations of those we process data about. Our activities reliant on legitimate interest are as follows:

a. **Employees:** We require the data processing to enable us to be a good employer and pay employees. Whilst they are candidates we require it to assess them for employment. Employees and candidates expect us to hold and process that personal data for those purposes. We destroy candidate personal data if the candidate is unsuccessful.

b. **Suppliers, and partners:** Our suppliers and partners are not usually individuals so here we are dealing with the identifiable employees of our suppliers and clients who require us to deal with such individuals or self employed individuals. We require their personal data (email, office address, telephone numbers) to enable us to contact them in the context of their job. If an employee leaves a client or supplier we remove their details from the CRM and other systems (or we would be communicating with the wrong person). They expect that we will hold their contact details for this purpose.

c. **Customers:** When individuals purchase products or utilise services through our trading company we have access to process this data to administer our contracted duties and send them carefully selected information about our products and services.

In all the above cases we believe that we have a legitimate interest in carrying out that processing and that the processing has no significant risk to the rights and freedoms of the individuals concerned.

8. Employees

We are satisfied that we only process employee Personal Data where we have a legitimate interest in so doing and are changing/have changed our contracts of employment and staff handbook to make this clear and include the necessary notices.

We hold next of kin/emergency contact details in respect of employees. This is authorised under Article 6.1 (d) GDPR as the processing is necessary to protect the vital interests of the employee.

9. Notices

As noted elsewhere we do not believe that GDPR should be interpreted as requiring an Article 13 or Article 14 notice to be sent to every data subject whose personal data we are processing. We do believe that such notices should be sent to:

- Suppliers and clients once engaged with Invincible Leisure Ltd
- Our employees

10. Processors

We have identified the following parties as data processors:

- Microsoft - In the provision of One Drive applications
- Xero - In the provision of accounting software
- Fatsoma - In the provision of ticketing services
- Aviva - In the provision of employee Pension Scheme

- HSBC - In the provision of PAYE and contractor payments
- ID Scan - In the provision of customer entry system

The above parties either have a direct contract using Invincible Leisure model contract or through GDPR compliant terms and conditions of use of service.

Appendix

Article 1 – Fatsoma Compliance Statement

Article 2 - Fatsoma Consumer Rights

Article 3 - Mailchimp Privacy Policy