September 2024

Jenningbet Customer GDPR Policy

Privacy Statement

At the Jenningsbet group, Jennings Racing Limited, Betting Shop Services Limited, Betting Shop Operations Limited, Megabet UK LTD and Mark Jarvis Limited we are committed to protecting and respecting privacy under the following brand **Jenningsbet**.

This privacy notice outlines our obligation and commitment based on General Data Protection Regulation (GDPR) and the principles held within them. It sets out what we will do with any personal data we hold about customers.

Personal data means data which relates to a living individual who can be identified –

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Controller

Jennings Racing Limited is the controller and responsible for your personal data (collectively referred to as "Company", "we", "us" or "our" in this privacy notice).
We have appointed a data privacy manager who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, including any requests to exercise your legal rights, please contact the data privacy manager using the details set out below.

What personal data do we hold on customers at Jenningsbet?

The customer data collected by Jenningsbet has a lawful basis so that the company can be compliant with our obligations in regards to The Gambling Act 2005, Proceeds of Crime Act 2002 and the Terrorism Act 2000. Under the Gambling Commission's Licencing Conditions and Codes of Practice (LCCP) 3.4

<u>Customer Data Collected to Prevent Crime and Disorder</u>

A monitored customer's betting data includes their name and betting activity such as dates of visits, stakes, turnover and losses. A copy of their transaction (bet) is assigned to each monitored customer's profile. Our monitored customer data is held via our secured till systems and each shop has access to their own monitored customer data. All monitored customer data is held securely and can be reviewed on a daily basis by authorised persons.

Any suspicious betting patterns, large stakes, accumulative losses or change in betting behaviour are reported to either the company MLRO or the compliance team for further investigation. Verification checks may be conducted with third party organisations, such as credit reference agencies. We may also conduct background searches and checks including information that is already in the public domain. Where applicable this may mean accessing the details of social media accounts.

On occasions certain customers will be asked to confirm their identity and/or show they have sufficient funds to support their gambling activity and that these funds have come from a legitimate source. The information provided will be treated in the strictest confidence in line with Data Protection requirements and the information provided will not be used for any other purpose. This information will be held securely at head office by the compliance team and will be retained in line with legal requirements currently 7 years.

Any significant winnings that a customer has requested to be paid by bank transfer are processed the same day as the request. For regulatory purposes a copy of their transaction (bet) is securely held on our server and the customer's data is electronically stored securely with the accounts department at head office. We do not hold the data or debit card details for any customers paying via debit card within branch this information is held by a third-party. For HMRC purposes this data is retained for 7 years.

If necessary, under our legal obligations monitored customer data will be provided to regulatory authorities and public bodies namely the Gambling Commission, HMRC, Police and the National Crime Agency (NCA). All monitored customer data is stored and retained for a period of 7 years and then destroyed.

<u>Customer Data Under Our Obligation To Protect The Vulnerable</u>

Obtaining knowledge of a customer provides us with information to help establish if they are potentially vulnerable to gambling related harm (GRH) and/or developing into a problem gambler. Further information regarding this obligation can be found in our Customer Interaction Policy. Customer data that is obtained and stored to ensure our compliance with social responsibility obligations contained in the LCCP includes, but is not limited to: customer's name, Nom Du Plume, betting patterns, observations regarding customer behaviours, knowledge about a customer's circumstances, self-exclusion arrangements and any other details that can be helpful in identifying GRH.

Gaming machine customer accounts data is held by our third-party supplier, who will, at its election and as necessary to enable Jenningsbet to meet its obligations under Data Protection Laws make such corrections, deletions, or restrictions on the company's behalf. To the extent a Data Subject's Personal Data is not accessible to Jenningsbet our supplier will, as necessary to enable Jenningsbet to meet its obligations under Data Protection Laws, provide reasonable assistance to make such Personal Data available to us.

This data is used as part of our player protection measures in line with the Betting and Gaming Council (BGC) Code of Conduct and LCCP 3.4 obligations. Our machine supplier uses a data algorithm to

measure customer behaviour from account based play, based on identifiable markers of harm allowing customers who may be at risk to be identified. Our supplier stores all customer account data securely and will communicate with Jenningsbet compliance team to identify at risk customers who may not be displaying obvious signs of, or overt behaviour associated with, problem gambling.

All aforementioned customer data in the prevention of GRH is recorded on our social responsibility platform (shopworks). This system is secure and access limited to relevant persons. The data is destroyed after 7 years.

Any customers subject to age verification (AV) checks will have their identification reviewed in branch at the time of entering the premises. The AV check will be recorded in accordance with regulatory requirements but the personal data is not recorded or held.

CCTV

CCTV systems are installed on our premises for the purpose of public and staff safety, crime prevention and detection and the abuse of Jenningsbet policies. In all locations signs are displayed notifying that CCTV is in operation.

We will only disclose CCTV images to others who intend to use the images for the purposes stated above. These images will not be shared with any other person or organisation, unless consent has been given or we are legally obliged to do so. CCTV images will not be released to the media for entertainment purposes or placed on the internet.

Images captured by CCTV will not be kept for longer than necessary. However on occasions there may be a need to keep images for longer for example where a crime is being investigated. The data is secure and accessible to only authorised persons. Shop staff have no access to the data stored but are able to view live images to assist with the day to day running of the business and the licensing objectives.

Customer Complaints

We keep a record of customers information when they write to us (by letter or email), such as name, address, email address, telephone number and details of their enquiry. This data is stored securely at our head office.

When customers call our Customer Service Team, telephone calls may be recorded. All callers are informed of this at the beginning of the call. Call recordings are kept for a period of 12 months after which time they are archived. All calls are deleted after a period of 7 years. Some of this information may have to be shared with our regulators such as the Gambling Commission, Advertising Standards Authority, Independent Betting Adjudication Service, and the Information Commissioners Office. This information will be retained in line with our retention policy.

Subject Access Request

Jenningsbet is committed to operating openly, transparently, and to meeting all reasonable lawful requests for information that are not subject to specific exemption in the Act. In the first instance all applicants should contact us at Dataprotectionmanager@Jenningsbet.com.

The following requirements must be met for a SAR to be valid:

a) The applicant must submit a written Subject Access Request

b) The applicant must supply two forms of identification: (1) Identification with a photograph and signature e.g. passport, and (2) Identification with proof of name and address e.g. a recent bank statement or utility bill (issued in the last three months)

c) The applicant must supply any further information that is reasonably required to assist us in locating information relevant to the request.

We will identify if any of the information gathered was provided by or identifies a third party. If we identify information that relates to third parties, we will take all reasonable steps to establish whether this information can be disclosed. We are not required to disclose information relating to third parties, unless they have provided their consent or it is reasonable to do so without their consent. If the third party objects to the information being disclosed, we may seek legal advice on what action we should take. Before sharing any information that relates to third parties, we will where possible anonymise information that identifies individuals not already known to the applicant. We will also edit information that may affect another party's privacy, and if necessary, summarise the information provided (rather than provide a full copy of the document).

We will respond to the request within 28 calendar days after accepting the request as valid. If the complexity or number of requests received means that additional time is needed or further information we may require an extension of up to 2 months.

Once we have confirmed identification, resolved any queries around the applicant's request, and gathered the relevant information, we will issue our response electronically via a secure email service, or if requested, via hard copy. Hard copy responses will be sent by Royal Mail recorded delivery in an envelope or package marked 'Private and Confidential' and 'Addressee only'.

Self-Excluders Agreements

Multi Operator Self Exclusion Scheme (MOSES) - Each MOSES self-excluder agreement is received over a secure network from MOSES and is password protected. The self-excluder's name, agreement expiry date and shops they have added to their exclusion are added to our central database secured in the compliance folder. Each self-exclusion form is then sent over our secured network to the relevant shop email address. All MOSES communication is via the email address selfexcluders@jenningsbet.com. This email account is accessible only by authorised persons and is password protected. When the shop team receive the form this is then printed and stored in the shop's compliance folder which is secure behind the staff counter which has restricted access.

Jenningsbet In-House Self Exclusion Agreements – These are completed in shop by the customer and signed off by a trained member of staff. The other hard copy is sent via Royal Mail to the compliance team in head office. This is then scanned and added to the in-house self-exclusion database within the compliance folder. A copy is then circulated to all shops on the agreement as chosen by the customer via the email address selfexcluders@jenningsbet.com. One hard copy is kept in shop and stored in the shop's compliance folder which is secure behind the staff counter which has restricted access.

The Self-Excluder form is then destroyed and their name removed from the central database six months after the expiry date of the agreement. Unless said customer requests to extend their agreement for one or more further periods of at least six months each. Our self-exclusion procedures

are in accordance with our obligations under the LCCP Social Responsibility Code 3.5. MOSES privacy policy can be found at https://self-exclusion.co.uk/terms-and-conditions.

Data Protection Manager

All GDPR and privacy queries should be sent for the attention of the data protection manager at Dataprotectionmanager@Jenningsbet.com.

Data Security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.
We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

Disclosure of personal data with third parties

Occasionally your data will be disclosed to third party organisations with whom we contract to provide services on our behalf. These services will only be carried out under contract which will contain our instructions and expectations in respect of how your data will be used. Information in relation to Suppliers and Contractors is used to manage the provision of goods and services to us. Depending upon the nature of the service, this may include the use of personal information.

Internal Third Parties

Other companies in associated with or internal to Betting Shop Services Limited.

External Third Parties

Service providers based in the UK or EEA who provide services on our behalf, including but not limited to:

1. Gaming and betting products.
2. Professional advisers including lawyers, bankers, auditors and insurers based in the UK or EEA who provide consultancy, banking, legal, insurance and accounting services.
3. HM Revenue & Customs, regulators and other authorities based in the UK or EEA who require reporting of processing activities in certain circumstances.
4. Agents, surveyors, valuers, insurers, councils and utility providers (if necessary) for contact purposes.
5. Contractors to complete emergency, responsive or planned property repairs.
6. Security system providers.

Changes to our GDPR policy

We may occasionally make changes to this document. It was last updated on 30th September 2024