Name of the policy **Privacy and Data Protection Policy**	
Written by ***Vincent Bezzina DPO***	***Written on*** **05 May 2020**
Updated by ***Filippo Pellicciari DPO***	***Updated on*** **09 September 2024**
Regulation ***GDPR, UK GDPR***	**Version Number** **1.1**
Date approved	**Approved By** **Board of Directors**

Policy Owner: DPO, Filippo Pellicciari

Review Cycle: Yearly

Applicability: All NetBet employees

Security Classification: Internal

Version Control:

Author	Date	Update	Version
Vincent Bezzina	05/05/2020		1.0
Vincent Bezzina	15/05/2020	Copy given to FIAU Malta	1.0
DPO Filippo Pellicciari	01/08/2024	Review	1.1
CTO Guillaume Raillard	02/09/2024	Review	1.1
Board of Directors		Approval	1.1

Table of Contents

1 Definition of Terms

Terminology	Explanation
GDPR	EU General Data Protection Regulation
UK GDPR	UK Data Protection Act 2018 Regulation
PII	Personal Identifiable Information
Data subject	The identified or identifiable living individual to whom personal data relates.
Data Controller	Entities or individuals that need to process personal data in order to do business. They determine the purposes for which and the manner in which the personal data is processed.
Data Processor	Processors take and/or process personal data on behalf of the Controller.
PIA	Privacy Impact Assessments.
DPO	Data Protection Officers.
DSAR	Data subject access requests.
PIA	Privacy Impact Assessments.
PCI	Payments Card Industry Security Standard.

2 Introduction

This document sets out the Data Protection Policy for NetBet. As an entity incorporated in Malta, Netbet is bound by the rules and regulations set out under the European General Data Protection Regulation and implemented by the various member states and applicable since 25th May 2018. which was introduced following Brexit and is based on the UK Data Protection Act 2018.

The GDPR is meant to unite and harmonize privacy laws across the EU, protect and empower EU citizens with data privacy, and will impose new requirements on organizations handling personal data

NetBet regularly monitors Data Protection regulations in each market operates such as the UK GDPR and ensure is always compliant. UK GDPR, which was introduced following Brexit and is based on the UK Data Protection Act 2018, is applicable to all organizations that process the personal data of UK residents. There is a recognition that personal information can be misused in ways which may lead to discrimination or manipulation of individuals. Personal details can be used to commit fraud with consequences for the persons whose identity abused. Even if securely held, there is still an issue of Privacy and Ownership of data. GDPR and UK GDPR makes it clear that individuals are entitled to privacy and that personal data belongs to the person.

Companies choosing to handle information have responsibilities which come with these activities.

Finally it should be remembered that GDPR and UK GDPR applies to data in any shape and form and is not limited in any way to the digital domain.

3 Personal Identifiable Information

The GDPR and UK GDPR respectively, applies to any organization that handles the personally identifiable information (PII) of EU and UK citizens, whether that organization is in North America, Europe, or somewhere else in the world.

PII is data kept by an organization which can be used to "distinguish or trace an individual's identity." PII could include names, birth dates, birth places, mothers' maiden names, addresses, emails, IP addresses, or social security/insurance numbers.

"Linked PII' is any information that is linkable to an individual, like educational, medical, employment, or financial information. PII also includes payment card details such as the magnetic card stripe (also known as track data) and primary account numbers (PAN).

4 Data Controller and Data Processor

GDPR and UK GDPR define different responsibilities according to two types of organization defined under GDPR and UK GDPR, these being a Data Controller and a Data Processor.

Under this definition, NetBet is a Data Controller; in turn NetBet shares a lot of data with many Data Processors who provide a multitude of services to NetBet.

5 Responsibilities under GDPR and UK GDPR

GDPR requirements	
Breach notification	Data controllers must report personal data breaches no later than 72 hours after they are aware of the breach.
Consent	Consent must be obtained from individuals for processing personal data.
Data Protection Officers (DPO)	Appointing DPOs will be mandatory for companies that are public authorities, process high volumes of personal data, or process special categories of personal data.
Data subject access requests (DSAR)	The time limit to comply with DSAR has been reduced from 40 days to one month.
Privacy by design	Products, systems, and processes must consider privacy-by- design concepts during development.
Privacy Impact Assessments (PIA)	PIAs must be carried out in certain situations.
Privacy notices	Privacy notices must be more transparent, using clear and plain language, and easily accessible.
Profiling	An individual has the right to not be subject to profiling, and profiling for marketing purposes will always require explicit consent.
Record keeping	Each data controller must keep a record of processing activities.
Right to portability	Users may request a copy of personal data in a portable format.

Right to erasure	Data subjects have the right to request for their data to be deleted.
Right to object	Individuals should be advised that they have the right to opt out of direct marketing

6 Lawful basis for processing

Netbet is required to process personal data only on when there is a valid lawful base. Lawful basis for processing are six and are listed in the GDPR and UK GDPR art.6.

Before starting any processing activity, we are required to determine the lawful basis, based on the single activity and this should be documented in the register of processing activity.

NetBet privacy notice, available on our website, includes our lawful basis for processing as well as the purposes of the processing.

Lawful base	Description
Consent	Individual has given clear consent for us to process their personal data for a specific purpose
Contract	Processing is necessary for a contract we have with the data subject, or because they have asked us to take specific steps before entering into a contract.
Legal obligation	Processing is necessary for us to comply with the law (not including contractual obligations).
Vital interests	Processing is necessary to protect someone's life.
Public task	Processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law
Legitimate interests	the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

7 Communicating Privacy Information

GDPR and UK GDPR has some core principles on communicating with those you obtain PII from. This could be directly to an individual who is giving you their PII or to an entity that provides you with previously collected PII.

These principles center around clear communication to data owners on what data you are getting, why you need it, and how it will be treated (including your data retention periods and how data will be deleted/destroyed). This communication is required to be transparent, using clear and plain language, and easily accessible to your customers. This communication will need to explain topics such as your lawful basis for getting their data, how long it will be kept, and what their rights are regarding the data you are processing or storing.

Existing Privacy information covering both NetBet's customers and internal data subject, can me modified without prior acceptance from PII, which still need to be promptly informed.

8 Individual's Rights

GDPR and UK GDPR sets clearly the individual's rights. These include:

Right to be informed	Data subjects have the right to know about the collection and use of their personal data
Right of access	Individuals have the right to access their personal data and verify the lawfulness of the data processing
Right of rectification	Individuals have the right to have their personal data rectified if it's inaccurate or incomplete.
Right to portability	Users may request a copy of personal data in a portable format that can be transferred to another entity (e.g., CSV file).
Right to erasure	Data subjects have the right to request for their data to be deleted.
Right to object	Individuals should be advised that they have the right to opt out of direct marketing.
Right not to be subject to automated decision-making including profiling	An individual has the right to not be subject to profiling, and profiling for marketing purposes will always require explicit consent

Exemptions to Individual Rights

It is important that GDPR and UK GDPR is not used as an excuse for poor record keeping, destruction of records or obfuscation whether instigated by the Individual or the organization.

NetBet is still subject to requirements brought about by Money Laundering Regulations and Financials Institutions to combat fraud and perform digital forensics.

There are therefore exemptions to individual rights with regards to keeping data beyond retention periods. NetBet can keep records for purposes of: IRS, HIPAA requirements, PCI requirements, or legal cases.

NetBet must therefore clearly identify cases where data is held beyond the retention period, which a clear justification for this retention; the use of this data must then strictly abide to the terms of use. This requirement must be clearly communicated across the company from development to database administrators, to application developers and business users with the organization.

9 Data Retention

NetBet complies with the GDPR and UK GDPR's principles related to data retention:

- Storage Limitation: Ensure personal data is not retained beyond the necessary time period
- Minimisation: Collect only the minimal amount of data required
- Accuracy: Maintain accurate, up-to-date, and reliable information

When processing PII Nebet ensures they are adequate, relevant and limited to what is necessary in relation to the specific purposes of the processing.

Necessity is a key factor in an effective data retention timeframe and is determined by your purpose for processing. Storage periods will depend on several elements, such as the industry sector, the type of data processing, and any other regulatory requirements that apply. However, in some circumstances there is a statutory retention. For example FIAU requires to maintain player's data for a minum period of 5 years after the account is closed and be extended up to 10 years.

To ensure effective data retention periods are in place NetBet has a data retention policy which provides an overview of the data management practices and is a broad document outlining how the organisation manages its data, how long it keeps certain types of data, and the roles and responsibilities of staff.

10 Security by Design

GDPR and UK GDPR places a big emphasis on security. NetBet adopts the Payments Card Industry Security Standard and Data security standard (PCI DSS) standard as this is the best security standard which addresses all the requirements under GDPR and UK GDPR. Others standards such as standards proposed by NIST in the USA are also considered. This means we make the use of scanning tools as well as manual scans to ensure these standards are assured. Also, NetBet technology is ISO/IEC 27001 certified.

In line with our Information Security Policy the following measures are in place:

An Information Security Policy must be implements and maintained
Penetration tests must be carried our regularly. Vulnerability scanning should also be run internally against specific software applications
Firewalls must be installed at all points to control both inbound and outbound traffic. Traffic should be further restricted to network zones.
Access must be restricted based on minimum permissions to carry out tasks
All access must be logged
Application development must take into accounts security

Encryption and Digest must be used to protect data
Data must be encrypted in Transit
Data must be archived or deleted when no longer required
Virus and Malware Detection Software must be installed on all computers. Servers should be further protected with intrusion detection systems (IDS).
Implement web application firewalls (WAFs) in front of public-facing web applications to monitor, detect, and prevent web-based attacks.
Ensure Remote Access uses strong authentication such as multi-factor authentication and proper firewall configuration.
Ensure Wireless Network is deployed securely. Wifi Traffic should be firewalled and with restricted access, backed by additional authentication factors.
Ensure Strong passwords policies around strength, sharing and changing of passwords.
Ensure Physical Security: Keep confidential information, products, or equipment in the workplace, secure these items in a locked area. Limit outsider access to one monitored entrance, and (if applicable) require non-employees to wear visitor badges at all times.
Employees should receive regular training about GDPR and security best practices.
Install File Integrity Monitoring on servers.
Ensure that all systems are properly patched and maintained or upgraded.

11 Subject Access Requests

Netbet must be able to comply with a data subject access request (DSAR) within one month.

Netbet is not able to charge individuals for complying with a request to access information under normal circumstances; Netbet can therefore refuse or charge for requests that are manifestly unfounded or excessive.

If Netbet refuses a request, Netbet must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. Such communications must also be done without undue delay, within one month of the refusal/charge.

DSARs can be made via any channel. DSAR need to be sent to the DPO mailbox: dpo@netbet.com, who will review the request and with the support of the CS team process the request.

A dedicated procedure for DSARs handling is implemented and owned by the DPO.

12 Data Breaches

A PII data breach is a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed. Supervisory authorities must be told within 72 hours of when the controller becomes aware of a data breach— where feasible, and unless the controller can demonstrate that the breach is unlikely to result in risk to the rights of the data subject. Controllers may also give reasons for delay, if applicable. If individuals face an adverse impact, you should contact individuals directly.

Nebet DPO is required to assess identified possible breaches and proceed with the classification, based on the following elements:

- Check if personal information is involved
- Establish what personal information has been breached
- Consider who might have the personal information
- Work out how many people might be affected
- Consider how seriously it will affect people
- Assess the risk in 3 categories (low, medium and high).

Failure to report a breach when required to do so could result in a fine, in addition to the fine for the breach itself.

13 Data Transfer

NetBet adheres to strict protocols for transferring personal data both within and outside the European Economic Area (EEA) and United Kingdom. This policy ensures that data protection standards are maintained consistently across all transfers.

For transfers of personal data to third-party companies within the EU or UK, we ensure that all parties comply with the applicable data protection regulations. Data Processing Agreements (DPAs) are in place with these entities to outline their obligations and ensure GDPR and UK GDPR compliance.

When transferring personal data to jurisdictions outside the EEA or UK that lack an adequacy decision by the European Commission or UK, we implement the following safeguards:

Data Processing Agreements (DPAs): We enter into DPAs with third-party vendors and partners who process personal data on our behalf. These agreements specify data protection requirements and ensure compliance with GDPR and UK GDPR.

Data Transfer Agreements (DTAs): For international transfers, we use Data Transfer Agreements incorporating Standard Contractual Clauses (SCCs) or other approved mechanisms. These agreements ensure that the recipient provides an adequate level of protection for the data.

14 Incident Response Phases

Nebet has implemented an incident response plan in line with our Incident Policy, Steps are based on the incident classification and prioritization is already defined and using our incident communication as well as our incident response team:

1. Prepare	Implement the many recommendations of this document to ensure security and compliance.
2. Identify	This can be internal detection, complaints from clients indicative of a breach of their data or being alerted by law enforcement.
3. Contain	Stop the breach without eliminating evidence
4. Eradicate	Remove the threat completely and eliminate vulnerabilities
5. Recover	Return systems to normal operation
6. Review	Forensic investigation and investigation

15 Data Mapping and Records of processing activities

Data discovery and mapping is a basic principle of all data security efforts; you can't protect what you don't know is there. Netbet DPO regularly conducts mapping exercise searching for PII with various tools, conducting interviews, reviewing documents, mapping software data flows, etc.

As part of its GDPR and UK GDPR compliance efforts, Netbet implemented its records of processing activities (ROPA). ROPA is owned by the DPO, and complies with requirements listed under art. 30 GDPR and UK GDPR and is subject to an yearly review to ensure entries are always correct and up to date.

Using this approach NeBet can establish what PII is received, where it flows and where it may be stored, being able to address risks and maintaining effective records.

16 Data Protection Impact Assessments

Data protection impact assessments (DPIA) are essentially a formal risk assessment process.

This risk assessment will use information gathered from the data mapping exercise as well as information about all the systems and networks used to process data.
This process is critical to implementing a "data protection by design and default" philosophy, which will be discussed later. In addition, any hardware, people, processes, and conditions that could represent a risk to this data processing will have to be evaluated. It would also potentially include risks for power loss or physical damage to a facility to be totally complete.

Necessity of performing a DPIA is assessed by the DPO also when there's a potential change in risk represented by new or changed processing operations, specifically to risks that might affect the rights and freedoms of data subjects, including:

- A new technology being deployed
- A profiling operation likely to significant impact individuals
- When there's large scale processing of special categories of data

Findings of the DPIA are ultimately presented to the board.

17 Data Protection Officers

NetBet has appointed a Data Protection Officer (DPO) to oversee the data protection practices and ensure compliance with GDPR and other relevant data protection regulations. The DPO is responsible for monitoring our data processing activities, advising on data protection obligations, and serving as a point of contact for data subjects and regulatory authorities. For any questions or concerns regarding data protection, including our data transfer policies and safeguards, please contact our DPO at dpo@netbet.com

18 Addressing Compliance to GDPR and UK GDPR

Netbet undertake the following actions to ensure compliance at all times with the accountability principle of the GDPR and UK GDPR:

- The legal basis for processing personal data is clear and unambiguous
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff. Internal trainings are delivered by the DPO to all new starters in the first month and regularly on a yearly basis.
- Rules regarding consent are followed
- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively
- Regular reviews of procedures involving personal data are carried out
- Privacy by design is adopted for all new or changed systems and processes
- The following documentation of processing activities is recorded:
    - Organization name and relevant details
    - Purposes of the personal data processing
    - Categories of individuals and personal data processed
    - Categories of personal data recipients
    - Agreements and mechanisms for transfers of personal data to non-EU countries including details of controls in place
    - Personal data retention schedules
    - Relevant technical and organizational controls in place

These actions are reviewed on a regular basis as part of the risk management process concerned with data protection.

19 Penalties for failed Compliance

Compliance with GDPR and UK GDPR is mandatory and fines set out below can be imposed for any breaches. As a condition of handling PII for EU citizens, Netbet is required to ensure that it has no poor security practices which might endanger personal information either collected by Netbet or Data Processors acting on behalf of Netbet.

The GDPR (EU) stipulates that an entity can face fines of up to €20 million or 4% of their global annual turnover (whichever is greater) for serious violations. Similarly, the UK GDPR imposes fines of up to £17.5 million or 4% of global annual turnover (whichever is greater) for the same serious violations, such as insufficient customer consent for data processing, breaches of the core principles of data protection, including "Privacy by Design and Default," and the unlawful processing of personal data.Both regulations also outline a tiered approach to fines:

- 2% of annual global turnover can be imposed for less severe infringements under both GDPR and UK GDPR. This includes failures such as not maintaining adequate records of processing activities, not notifying the supervisory authority and data subjects of a data breach within the required timeframe, and failing to conduct a Data Protection Impact Assessment (DPIA) when necessary.

It is important to note that these fines apply to both controllers and processors; for example, data cloud services will not be exempt from GDPR and UK GDPR enforcement.