DATA PROTECTION POLICY

SAFEGAURDING OUR CLIENTS' SENSITIVE DATA

CONTENTS

1. INTRODUCTION - SCOPE

The following Policies and Procedures are derived from the European Union's General Data Protection Regulations and put in place by Blueberry Payment Solutions (BPS) to enforce the protection of our clients' personal data in regard to:

- Processing of personal data.
- Transference of personal data.
- Secure storage of personal data.
- The execution of automated processing of personal data.

2. THE PROCESSING OF PERSONAL DATA

2.1 GOVERNING PRINCIPALS

PURPOSE LIMITATION – DATA MINIMIZATION

All data requested by BPS from our users will be relevant and limited to what is necessary for both parties to enter into a legitimate Business Relationship. We are committed to data minimization, to avoid the over capture of data.

ACCURACY OF DATA

Incorrect data that has been received by BPS will be erased or rectified without delay to ensure that all processed data remains accurate and without error. This policy is also relevant for data that requires periodic updating (i.e Proof of Address) or if a data item becomes outdated/expired (i.e Proof of Identification).

STORAGE LIMITATION

Captured data will be stored no longer than is legally or operationally required.

INTEGRITY & CONFIDENTIALITY

Archived digital and Physical Personal data will be protected at all times against unauthorized or unlawful processing and against accidental loss, destruction or damage.

ACCOUNTABILITY

Access to Personal Data will be recorded to ensure that any unauthorized access can be detected, and accountability and responsibility can be assigned to the relevant party.

LEGAL OBLIGATION TO PROCESS DATA

As BPS offers financial services to individuals in the general public, we have a legal obligation to request personal data in order to verify the true legal identity of the natural persona as well as other relevant data points. All data is requested prior to entering a business relationship.

3. LEGAL RIGHTS OF THE DATA SUBJECT

All participating individuals will have the right to request access to their data. This request can be submitted for a variety of reasons. BPS has outline ways in which natural persons can gain access to certain personal data, in a controlled and timely manner.

3.1 PERSONAL DATA CAPTURE TRANSPARITY

In order for a customer to be successfully onboarded they will have to complete a series of questionnaires and provide information to verify their Identity, physical address and potentially some financial information. All information will be compiled into a Customer Identification File (CIF). Upon capture of personal information, BPS discloses the following:

- Contact Details of the Company.
- The Legal necessity for the capture of this data.
- The Period of which the personal data will be stored (Legal requirement of 7 years).
- The right to request access to the data captured for:
    - Rectification
    - Deletion
- The right to lodge a complaint with a supervisory authority.
- The disclosure of any automated decision making based on submitted data. (i.e risk-based scoring for the customer profile).
- State that this data is for internal compliance purposes only.

3.2 RIGHTS OF ACCESS

The data subject has the right to obtain access to the personal data they have submitted and to receive confirmation of the reason their data is being processed. The following information will be provided on request:

- The reason and purpose of the data that is captured.
- The Period of which the personal data will be stored (Legal requirement of 7 years).

All Personal information captured by BPS is declared by the data subject. Upon completion of the registration process, BPS customers will be able to log into their website and access all this personal information via their “Profile Page”.

3.3 RIGHT TO RECTIFICATION

BPS users will be able to edit and rectify all submitted personal data at their own discretion by accessing their profile page within the Blueberry website or mobile application. However, it must be noted that rectifications are subject to a review by a compliance officer to ensure the legitimacy and accuracy of the personal data captured. Additional information may be requested once an individual has rectified a personal data item.

3.4 RIGHT TO ERASURE

As BPS offers financial services the legal requirements to store physical and digital data override any requests to delete submitted data prior to the 7-year archiving period. This is clearly stated within the onboarding procedure, prior to entering a business relationship with BPS.

4. PROCESSING PERSONAL DATA

The processing of personal data is described as any process or operation that involves the usage/transference of personal data. Blueberry's sole processing activity commences upon the submission of personal data by the data subject. This information is compiled and archived by means an automated technology that was built and maintained in house and therefore is the sole processor involved.

4.1 KEEPING A RECORD

As all processing is done with a technical aid and no manual intervention. A record will be kept electronically of the data subject's access, rectification, and addition of their personal data.

Once personal data has been submitted, our software will record each field of data into its respective category within the Blueberry database.

4.2 SECURE PROCESSING

As aforementioned all processing is done within our technical systems. Our IT Security Policy is based around the PCI DSS framework to ensure the highest standard of Technical and Access security is enforced by BPS.

For a full review of Blueberry's Data Security Standards please refer to IT_Security_Policy_V2.

4.2.1 IT SECURITY POLICY OVERVIEW

- Secure Network and Systems
- Secure Access to Networks
- Protecting Stored Cardholder Data (Personal Data)
- Secure Cardholder Data Across Open, Public Networks
- Protection Against Malware
- Secure Web-Based and Mobile Applications
- Strong Access Control
- Authentic Access to Internal Systems
- Restricted Physical Access
- Monitor Access
- Test Security
- Maintenance of IT Security Policy

4.3 PERSONAL DATA BREACH (PDB)

A personal data breach is described as a breach in security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, personal data. Blueberry exercises the highest standard to data security to mitigate this risk as much as possible, however impenetrable security is never guaranteed. The following policies are outlined to ensure a timely and effective response in the event of a personal data breach.

4.3.1 NOTIFYING THE SUPERVISORY AUTHORITY

After becoming aware of a Personal Data Breach Blueberry will without undue delay notify the applicable Supervisory Authority based on the member state that best observes the rights and freedoms of the data subjects effected by the breach.

When notifying the supervisory authority, the following will be expressed (if possible):

- The nature of the personal data breach.
- The nature of the data that was compromised.
- The number of data subject affected.
- Possible consequences of breach.
- What immediate action was taken to counter the breach.
- Name and contact details of the data protection officer.

All information will be submitted and recorded without undue delay. If this period exceeds 72 hours, further explanation will be provided.

4.3.2 NOTIFYING THE DATA SUBJECT

If a PDB occurs all effected data subjects will be promptly notified in order to minimize any adverse effects that could be caused by the breach. As Blueberry provides financial services, all personal data breaches will be considered high risk.

The communication will clearly express the following:

- Possible consequences of breach.
- What immediate action was taken to counter the breach.
- Name and contact details of the data protection officer.

Scenarios where data subject is not obliged to be notified:

- A breach occurred but the sensitive data was not compromised due to the use of encryption, truncation, masking, hashing or any other data defense material.

5. DATA PROTECTION OFFICER (DPO)

5.1 DESIGNATION

Person	**Role**	**Responsibilities**
Rhyan Bridle	Chief Technology Officer	Responsible for approval of IT security policies. Control of employee's system access, the domains they can access. Maintenance of the Server room.
Andreas Hadjiantoniou	Head of IT Security Data Protection Officer	Overall enforcement of security policies. Training of Staff. The semi-annual audit of the policies and implementation of new security measures. The first responder to any incident that causes the technological infrastructure to be compromised. Correspondence with data subjects

6. CODE OF CONDUCT

Blueberry has outlined a code of conduct to encourage the proper application of safeguarding processes in terms of Personal Data Capture and Processing. This code of conduct will apply to all current practices and should be considered when a new process is being designed to ensure future compliance with all GDPR and PCI DSS Regulations.

6.1 THE CODE

1. All processing of personal data should be done in a transparent manner.
2. Collecting of Personal Data must be done with the Data Subjects consent and must be made fully aware of the purpose of capturing this data.
3. Efforts should be made to ensure Data Subjects are aware of their rights and freedoms.
4. No data of persons under the age of 18 should be processed.
5. Data Subjects need to be notified if a harmful data breach occurs.
6. Controls and safeguards should be put in place to avoid all unauthorized access as best as possible.
7. Ensure that all personal data security is fully PCI DSS Compliant.
8. Yearly training should be given to all employees who are involved in the control or processing of personal data. To ensure the most contemporary measures are applied.

7. PERSONAL DATA TRANSFER (3RD COUNTRIES)

The transfer of personal data should be given the utmost care, to prevent access from unauthorized parties and to ensure the ongoing integrity of the data that has been transferred. Therefore, when transferring data, a full adequacy review of the destination should be undertaken and only if the destinations standards match that of the original controller should the data be transferred.

This risk is compounded when transferring data to 3rd Countries and therefore requires more stringent measures. Refer to the EU website to view a contemporary list of “3rd countries”.

https://ec.europa.eu/food/animals/movement-pets/eu-legislation/listing-territories-and-third-countries_en

7.1 ADEQUACY CRITERIA

- General climate of the Country in question
    - Rule of Law – Human rights, fundamental freedoms
    - The Political and Legislative regulation
        - Focus on Personal Data Protection Laws
    - The presence of Supervisory Authorities
        - Compliance and Enforcement

  - Presence of sanctions and adverse media

These reviews should be periodic as the Political and therefore legislative climate of the country is ever changing.

7.2 TRANSFER SAFEGAURDS

To safeguard against any misuse or unauthorized use of personal data that has been transferred one or more of the following safeguards should be enforced.

- A legally binding standard data protection agreement between both entities.
- A binding commitment to replicate Data protection principles of Blueberry.
  - Proof of the application of these principles
- Approval and advise from a Supervisory Authority.
  - Can be in the form of an approval code.
- An approval certificate from a third country Supervisory Authority that has adequate enforcement rights regarding data subjects' rights and freedoms.

Note: At the time of approval () Blueberry does not operate outside of EU member states who are not on the 3rd party list and have no current plans to extend beyond this jurisdiction. As and if this changes this section will be reviewed and updated.

8. COOKIE POLICY

8.1 INTRODUCTION

Blueberry may use cookies, web beacons, tracking pixels, and other tracking technologies when an individual visits our website www.blueberrycard.eu, including any other media form, media channel, mobile website, or mobile application related or connected thereto (collectively, the " Site") to help customize the Site and improve your experience.

We reserve the right to make changes to this Cookie Policy at any time and for any reason. Any changes or modifications will be effective immediately upon posting the updated Cookie Policy on the Site, individuals will not receive specific notice of each such change or modification.

Users are encouraged to periodically review this Cookie Policy to stay informed of updates. You will be deemed to have been made aware of, will be subject to, and will be deemed to have accepted the changes in any revised Cookie Policy by their continued use of the Site after the date such revised Cookie Policy is posted.

8.2 USE OF COOKIES

A “cookie” is a string of information which assigns a user with a unique identifier that BPS stores on your computer. Your browser then provides that unique identifier to BPS each time you submit a query to the Site. We use cookies on the Site to, among other things, keep track of services individuals have used, record registration information, record an individual’s user preferences, keep them logged into the Site, facilitate purchase procedures, and track the pages they visit.

8.3 TYPES OF COOKIES

The following types of cookies may be used on the BPS WebSite: www.blueberrycard.eu

ADVERTISING COOKIES

Advertising cookies are placed on an individual’s computer by advertisers and ad servers in order to display advertisements that are most catered to the specific induvial. These cookies allow advertisers and ad servers to gather information about users visits to the Site and other websites, alternate the ads sent to a specific computer, and track how often an ad has been viewed and by whom. These cookies are linked to a computer and do not gather any personal information about BPS Users.

ANALYTICS COOKIES

Analytics cookies monitor how users reached the Site, and how they interact with and move around once on the Site. These cookies let us know what features on the Site are working the best and what features on the Site can be improved.

OUR COOKIES

Our cookies are “first-party cookies”, and can be either permanent or temporary. These are necessary cookies, without which the Site won't work properly or be able to provide certain features and functionalities. Some of these may be manually disabled in your browser but may affect the functionality of the Site.

PERSONALIZATION COOKIES

Personalization cookies are used to recognize repeat visitors to the Site. We use these cookies to record your browsing history, the pages you have visited, and your settings and preferences each time you visit the Site.

SECURITY COOKIES

Security cookies help identify and prevent security risks. We use these cookies to authenticate users and protect user data from unauthorized parties.

SITE MANAGEMENT COOKIES

Site management cookies are used to maintain an individual's identity or session on the Site so that they are not logged off unexpectedly, and any information that is entered is retained from page to page. These cookies cannot be turned off individually, but all cookies can be disable in your browser.

THIRD-PARTY COOKIES

Third-party cookies may be place on your computer when you visit the Site by companies that run certain services we offer. These cookies allow the third parties to gather and track certain information about you. These cookies can be manually disabled in your browser.

8.4 CONTROL OF COOKIES

Most browsers are set to accept cookies by default. However, individuals can remove or reject cookies in your browser's settings. We make our users aware that such action could affect the availability and functionality of the Site.

For more information on how to control cookies, check your browser or device's settings for how you can control or reject cookies, or visit the following links:

8.5 OTHER TRACKING TECHNOLOGY

In addition to cookies, Blueberry may make use web beacons, pixel tags, and other tracking technologies on the Site to help customize the Site and improve our user's experience. A "web beacon" or "pixel tag" is tiny object or image embedded in a web page or email. They are used to track the number of users who have visited particular pages and viewed emails and acquire other statistical data. They collect only a limited set of data, such as a cookie number, time and date of page or email view, and a description of the page or email on which they reside. Web beacons and pixel tags cannot be declined, individuals can elect to minimize/limit their usage.