GLOBAL PRIVACY POLICY (GDPR)

KBJ PAY IS THE TRADING NAME OF KBJ SP Z.O.O., REGISTERED IN THE ENTREPRENEURS OF KRS KEPT BY THE DISTRICT COURT KRS: FOR THE CAPITAL CITY OF IN WARSAW, XII COMERCIAL DIVISION OF THE NATIONAL COURT UNDER KRS NUMBER 0000897043 REGISTRATION NUMBER 11650131

WE CARE ABOUT YOUR PRIVACY

A. KBJ Pay with its registered seat in Ł ul. Piekna 24/26A, 00-549 Warsaw, Republic of Poland (hereinafter: "the Company"), is legal entity incorporated by law of Republic of Poland and entered into Commercial Register under KRS Number: 0000897043 Registration number 11650131

B. As a business headquartered in Europe, we are subject to strict privacy regulations (among which, the European General Data Protection Regulation[1] and The Personal Data Protection Act of 10 May 2018[2]) that require us to comply with a number of obligations regarding your data (protection, retention, deletion, access rights).

C. The Company is strongly committed to protecting personal data. In this document, you, our Customer, can learn everything about how we use your data: that we collect it from you and your actions, that we process only what we need in order to perform what you have asked or consented to (or what the law requires us to), that we protect with appropriate technology.

D. We may also disclose personal information under the following circumstances:
   (1) with professional advisers, for example, law firms, as necessary to establish, exercise or defend our legal rights and obtain advice in connection with the running of our business - personal data may be shared with these advisers as necessary in connection with the services they have been engaged to provide;
   (2) when explicitly requested by you;
   (3) when required to deliver publications or reference materials requested by you;
   (4) when required to facilitate conferences or events hosted by a third party;
   (5) to law enforcement, regulatory and other government agencies and to professional bodies, as required by and/or in accordance with applicable law or regulation.

E. The Company may also review and use your personal information to determine whether disclosure is required or permitted.

F. Your local law may require us to set out in this privacy statement the legal grounds on which we rely in order to process your personal information. In such cases, we rely on one or more of the following processing conditions:
   (1) our legitimate interests in the effective delivery of information and services to you and in the effective and lawful operation of our businesses and the legitimate

[1] https://gdpr-info.eu/

[2] https://uodo.gov.pl/en/660/1464

interests of our clients in receiving services from us as part of running their organisation (provided these do not interfere with your rights);

(2) our legitimate interests in developing and improving our businesses, services and offerings and in developing new technologies and offerings (provided these do not interfere with your rights);

(3) to satisfy any requirement of law, regulation or professional body of which we are a member (for example, for some of our services, we have a legal obligation to provide the service in a certain statutory way);

(4) to perform our obligations under a contractual arrangement with you; or

(5) where no other processing condition is available, if you have agreed to us processing your personal information for the relevant purpose.

G. The right to privacy is a fundamental human right. We respect yours and make every effort to protect it.

H. Your Privacy Rights under GDPR:

- **Right to access**
- **Right to rectification**
- **Right to be forgotten**
- **Right to object to processing**
- **Right to restriction of processing**
- **Right to data portability**
- **Right to withdraw consent**

For further details regarding your Privacy Rights please refer to **Section 5.**

"HOW CAN YOU EXERCISE YOUR DATA SUBJECTS RIGHTS? " _

1. WHAT PERSONAL DATA DO WE COLLECT?

We can collect your data directly (e.g. when you give it to us), indirectly (e.g. when someone else gives it to us) or through automated technologies (e.g. cookies).

Please find below an outline of the types of data that we may collect and how we collect it.

Data Directly Provided To You	
Type of Data	**Description**
Basic identification data	E-mail address, Phone number
KYC customer data	Name, Address, Date of birth, Nationality, Country of residence, Government-issued identity document (e.g. passport, driver's license, or state identification card),

	Social security number, Employment information (e.g. company name), Proof of residency (including visa information), Utility bills – bank statement (for your billing address), Photographs and/or videos (if applicable), Income/net assets/wealth verification statements (if applicable), Criminal offences and allegations (EDD measures, if applicable), Family members and their professional roles (EDD measures, if applicable)
Professional Data	Employer Identification Number/ Social Security Number (or comparable number issued by a government), Personal identification information for all material beneficial owners of your business, employer, and professional role (if applicable).
Financial Data	Tax identification number, Income/net assets/wealth verification statements (if applicable)
Wallet Data	Wallet address, Wallet provider.
Account Data	Account provider, Account number.
Transaction Data	Data about the transactions made on our Websites and App, such as the amount, currency preferences, payment method, date, and/or timestamp, products purchased.
Customer Support Data	Data provided by you during customer support exchanges, or in response to customer surveys.
Biometric Data	We may collect biometric data if (and only if) voluntarily provided by you in the context of an identification verification procedure. We do so by collecting a live selfie that is compared to the photography of the identity provided by you. We use our software provider to process and store this data, and we do it to ensure that the person submitting the documents is indeed the owner of the documents, thereby increasing the level of safety and reliability of the verification. We do this with your express specific consent, given by you before the identity verification. You are also in full control of how and when the collection takes place. This data is used solely for this purpose, in the context of the anti-money laundering policy of the Company.
Behaviour and preferences	We observe how you use our website and Services, what features you like, and how you respond to our marketing efforts. This information is used to improve our Services, for you to have a better user experience, and to recommend features that might interest you, identify your preferences, and personalise your experience with the Services (i.e. preferred products, settings and preferences selected in Websites and/or App).
Special Categories of Data	These special categories include data about your race, ethnic origin, political opinions (if by an accident uploaded), religious or philosophical beliefs (if by an accident uploaded), trade union

	membership (if by an accident uploaded), health, biometric or genetic data((if by an accident uploaded), sex life or sexual orientation (if by an accident uploaded), and criminal convictions and offences (even if only suspected). We may need to process this type of sensitive data in the course of providing our services, but we will only do so in accordance with data protection laws and regulations, or if you give us your express permission to do so. It should be noted that this information could pose a greater risk to your fundamental rights and freedoms, as it could lead to unlawful discrimination. If we do hold this type of information because you've included it in the documents you've given us, we will rely on the substantial public interest condition set out in the Data Protection Regulations.

Data Indirectly Obtained About You	
Type of Data	**Description**
Basic information data, KYC customer data, Business and professional data, Financial data, Wallet data, Transaction data, Customer Support data	Described above. During your interactions with our affiliates, partners or service providers, you may provide them with data that may be transmitted to us for the purposes outlined below on "Why do we process your personal data". We may also receive data about you from a person who has submitted it for our referral program.
Publicly available data.	May include all types of data described above, if they are publicly available, as well as blockchain data, including timestamps of transactions or events, transaction IDs, digital signatures, transaction amounts, and wallet addresses unrelated to your transactions with us, as well as media reports about you. We collect and process publicly available data about you, as necessary for the purposes outlined below on "Why do we process your personal data".
Advertising Data	We receive data from our advertising partners on your interactions with marketing and advertising content (clicks, actions, time spent, etc.).
Analytics Data	We receive data from our analytic providers about your usage of the Websites and App (page clicks, actions, time spent, etc.), your age group and geographic region, as well as survey responses.

Counterparty Data	We may receive data from counterparties with whom you have interacted in relation to a Product or service provided by us, about how you have interacted with them.
Transaction Data	We may also receive transaction data from third-parties with whom we offer products to you with, such as the Company Card. In this case, the Company will receive data on your card usage, with the sole purpose of enabling you to see that data on your account.

Data Automatically Obtained About You	
Type of Data	**Description**
Device, browser and app data	Our systems collect information about your device, its operating system, and browser, along with additional features or identifiers such as plugins and the network you connect to, as well as your IP address.
Usage Data	Our plugins and cookies collect information about your activities, such as what you view or click on our Sites and Apps, your usage of our Services, as well as diagnostic and troubleshooting data, which includes service-related performance details, timestamps, crash data, website performance logs, and any error messages or reports.
See below provisions regarding "Cookies" _for more information.	

2. WHY DO WE PROCCESS YOUR PERSONAL DATA?

We use your personal data for different purposes, as indicated below:

Purpose / Activity	**Type of Data**	**Lawful basis for processing including basis of legitimate interest**
To open and maintain your account/ wallet	(a) Basic information data (b) KYC customer data (c) Professional data (d) Biometric data	(a) To perform a contract with you. (b) Necessary to comply with any legal obligation. (c) Necessary for our legitimate interests (to establish an ongoing customer relationship). (d) Which you expressly consent to when you create an account/ wallet.

To sell you the Products and provide you with services	(a) Basic information data (b) KYC customer data (c) Preferences data (d) Wallet/ Account data (e) Transaction data	(a) To perform a contract with you. (b) Necessary to comply with any legal obligation. (c) Necessary for our legitimate interests (to establish an ongoing customer relationship). (d) Which you expressly consent to when you create an account/ wallet.
To manage the Company store	(a) Preferences data (b) Transaction data (c) Customer support data	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganization or group restructuring exercise). (b) Necessary to comply with a legal obligation. (c) You expressly consent to this when you create an account/ wallet.
For advertisement, data analytics and to provide recommendations	(a) Analytics data (b) Advertising data (c) Device, browser and app data (d) Usage data (e) Counterparty data	(a) Necessary for our legitimate interests (to study how users use our services and website, to develop them, to grow our business and to inform our marketing strategy). This data is not shared/sold to third parties for any purpose whatsoever. (b) You expressly consent to this when you create an account/ wallet.
To comply with internal and external policies, guidelines, rules and legislation (for example, to respond to law	(a) Basic information data (b) KYC customer data (c) Professional data (d) Transaction data (e) Wallet data (f) Financial data (g) Publicly available data	(a) Necessary to comply with a legal obligation. (b) Necessary for our legitimate interests (ensure that we run a safe and credible platform).

enforcement requests)	(h) Counterparty data (i) Device, browser and app data	

3. WHEN DO WE SHARE YOUR INFORMATION?

3.1. General

- **We take the privacy of our users' personal information very seriously.**
- **We only share it as described here and with our subsidiaries or affiliates who either follow this privacy policy or adopt practices that provide at least the same level of protection as our safeguards.**
- **We work with various third parties to help us provide our services to you. These parties need access to your personal information to help us provide our services and comply with our legal obligations. These third parties help us with things like data analysis, marketing support, payment processing, content delivery, credit risk management and identity verification. You can be assured that we will only share your information with them after ensuring that they have robust security measures in place to keep your information safe.**

Our team and our group Your data may be accessed by our employees and people who we may hire as contractors or freelancers. Your data may be shared, with other entities of the Company Group if you wish to acquire Products that are sold by other entities of the group (if applicable).	The Company, other companies from the group, each labeled accordingly, when acquiring Products that are sold by this entity (Basic information data, KYC data, Account/ Wallet data, Financial Data, Transaction Data).
Our third-parties Your data may be received from, or shared with (to the extent necessary), the following entities that provide services to/with the Company, among others that the Company from time to time engages to provide services.	Your data may be shared with our third party partners, as instructed or needed in order to complete the services to you. The parties we share data with can include: Fraud monitoring and identity verification service providers Payment service providers IT and cybersecurity service providers Companies that offer services that complement our own

	Any person or organisation you've given us permission to share with We do not have a general list of all the third parties with whom we may share your information because it depends on how you use our services. However, if you would like more information about this or a list specific to you, you can contact us at info@kbjpay.com
Your Third Parties	Your data may be shared with your third parties, as instructed or needed by you, in order to complete the services to you. This may include your wallet/ account providers, your e-mail provider or others you may require us to engage with.
Public authorities and regulators, professional advisors and other industry partners	Your data may be shared with regulators and law enforcement authorities as per 3.2 below, in response to legitimate requests made in the course of their activity. Your data may also be shared, from time to time, with professional advisors such as lawyers, cybersecurity or compliance consultants, to fulfil our compliance obligations, assist us in defining adequate courses of action, and detect, investigate or prevent illicit activity in our platform.
Corporate Events	Your data may be shared in the context of a corporate event such as a purchase or sale of assets or of a company, a merger or spin-off, an acquisition or reorganisation, a liquidation or a simple change of control.

3.2. Specifically: Cooperation with law enforcement

Your personal data will only be disclosed to law enforcement authorities, courts or other government bodies, to the extent required by laws and regulations.

The Company does not normally disclose personal information about customers unless required to do so by an appropriate legal instrument (e.g., a subpoena, warrant, or the legal equivalent in the issuing country). Exceptional circumstances (such as a very urgent request that may save a person's life or prevent great harm) may dictate a different response on our part, but only to the extent permitted by law and only in the scenario where we are unable to contact you before making such a disclosure.

3.3. Specifically: Company Card

Certain Products may be offered, from time to time, together with third-party providers that may require the Company to process your personal data in order to provide it.

This is the case, for example, of the personal data collected in the context of the Company Card.

The joint data controllers for personal data connected with this product, which may include Basic information data, KYC customer data, Business and professional data, Financial data, Wallet/ Account data, Transaction data, and Customer Support data.

As a rule, the Company processes such data only as a data processor. This includes, specifically, data on the purchases you make with the Company Card. This information is passed to the Company from the joint data controllers for the sole purpose of showing it to you on your transaction history and is not processed for any other purpose.

However, the Company also acts as a data controller with respect to some of the data processed in connection with the Company Cards, e.g., where the Company processes personal data that is not processed by third-party data controllers (such as the password of your account) or where the Company processes personal data for the functions entirely handled by the Company (such as customer support, or to provide you with account management tools).

These are the relevant details for the processing of data in the context of the Company Card:

Purpose	1. To provide the Company Card according to the Terms and Conditions; 2. To monitor and store cardholder transactions in accordance with requirements provided for in the rules, procedures, laws and regulations that are designed to prevent money laundering crimes.
Categories of Personal Data	(a) Basic information data (b) KYC customer data (c) Professional data (d) Transaction data (e) Wallet/ Account data (f) Financial data (g) Publicly available data (h) Device, browser and app data

	(i) Counterparty data (including your transaction history with the Company Card)
Categories of data subjects	Potential and/or existing Customers.
Processing operations	Ordering and issuing the Company Cards by using Personal Data received from the Data Controllers. The provision of payment services as a, or on behalf of a, payment institution. Behaviour factor generation with respect to the transactions with Cards and the return of such information (reports) to the Data Controller, according to the Agreement. Keeping Personal Data as long as it is necessary to fulfil the objectives of the Agreement, or other agreements to be concluded between the Parties or fulfilling its obligations under the applicable law; improvement of the product and development of new tools related thereto.
Retention requirements	As long as it is necessary to fulfil the objectives of the Company Card agreements, concluded or to be concluded with you, or fulfilling their obligations under the applicable law.

4. HOW DO WE PROTECT YOUR PERSONAL DATA?

4.1. We are committed to protecting the privacy and confidentiality of your personal data. Access to your data is limited only to authorised the Company officers, employees, contractors or others who may require access to it in order to perform the services requested by you.

4.2. We have security measures in place to protect our and our clients' information (including personal data), which involve detecting, investigating and resolving security threats. Personal data may be processed as part of the security monitoring that we undertake. We monitor the services provided to clients for quality purposes, which may involve processing personal data stored on the relevant client file. We have policies and procedures in place to monitor the quality of our services and manage risks in relation to client engagements. We collect and hold personal data as part of our client engagement and acceptance procedures. As part of those procedures we carry out searches using publicly available sources (such as internet searches and sanctions lists) to identify politically exposed persons (PEPs), their family members (FMs) and known close associates (KCAs) and heightened risk individuals (as High Net-Worth) and organisations and check that there are no issues that would prevent us from a particular client (eg. sanctions).

4.3. More specifically, we have implemented the following security measures:

(1) Staff dedicated to cyber and physical security, that designs, implements and provides oversight to our information security program.

(2) The use of specialised technology such as host-based security tools, network defence monitors, and intrusion detection systems.

(3) Testing of the security and operability of products and services before they are introduced to the Internet, as well as ongoing scanning for publicly known vulnerabilities in the technology.
(4) Internal and external reviews of our Internet website and services.
(5) Monitoring of our systems infrastructure to detect weaknesses and potential intrusions.
(6) Implementing controls to identify, authenticate and authorise access to various systems or sites.
(7) Protecting information during transmission through various means including, where appropriate, encryption.
(8) Providing the Company personnel with relevant training and continually updating our security practices in light of new risks and developments in technology.

5. HOW CAN YOU EXERCISE YOUR DATA SUBJECTS RIGHTS?

5.1 You may have certain rights under GDPR law in relation to the personal information we hold about you. In particular, you have a legal right to:
(1) a

5.2 Rights of the individual:

A. The right to delete your personal data in the following cases ("Right to be forgotten"):
(1) the personal data is no longer necessary in relation to the purposes for which they were collected and processed;
(2) our legal ground for processing is consent, you withdraw consent and we have no other lawful basis for the processing;
(3) our legal ground for processing is that the processing is necessary for legitimate interests pursued by us or a third party, you object to the processing and we do not have overriding legitimate grounds;
(4) you object to processing for direct marketing purposes;
(5) your personal data has been unlawfully processed; or
(6) your personal data must be erased to comply with a legal obligation to which we are subject.

B. The right to restrict personal data processing in the following cases:
(1) for a period enabling us to verify the accuracy of personal data where you contested the accuracy of the personal data;
(2) your personal data have been unlawfully processed and you request restriction of processing instead of deletion;
(3) your personal data are no longer necessary in relation to the purposes for which they were collected and processed but the personal data is required by you to establish, exercise or defend legal claims; or
(4) for a period enabling us to verify whether the legitimate grounds relied on by us override your interests where you have objected to processing based on it being necessary for the pursuit of a legitimate interest identified by us.

C. The right to object to the processing of your personal data in the following cases:
(1) our legal ground for processing is that the processing is necessary for a legitimate interest pursued by us or a third party; or

(2) our processing is for direct marketing purposes.

D. The right to data portability.

The right to receive your personal data provided by you to us and the right to send the data to another organisation (or ask us to do so if technically feasible) where our lawful basis for processing the personal data is consent or necessity for the performance of our contract with you and the processing is carried out by automated means.

E. The right to withdraw consent.

Where we process personal data based on consent, individuals have a right to withdraw consent at any time. We generally try not to process personal data based on consent (as we can usually rely on another legal basis).

F. Right to access.

You can request access to your personal data. This enables you to receive a copy of the personal data we hold about you and to verify that we are lawfully processing it.

G. Right to rectification.

You can request correction of the personal data we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected. We may need to verify the accuracy of the new data you provide to us.

If you consider that the processing of your personal data infringes the law, you may have the right to lodge a complaint with the data protection regulatory authority responsible for enforcement of data protection law in the country where you normally reside or work, or in the place where the alleged infringement occurred.

if you have purchased Products that require KYC or if you have exhibit suspicious behaviour in your dealings with the Company. In some cases the Regulator (GIIF now, then Commission of Financial Supervision) may ask us to extend the retention time for certain data for another 5 years.

We will keep information that is relevant for tax purposes for up to 10 years.

6. HOW LONG DO WE KEEP YOUR PERSONAL DATA?

We will keep your personal data for the time needed to fulfil the purpose for which it was collected, be it selling you Products, complying with legal obligations, or protecting ours, yours or other's interests.

If you have an account/ wallet with us, we will keep your data collected in relation to your account/ wallet activity for as long as the account/ wallet exists.

We will keep information that is collected and processed for compliance purposes (namely information connected with ongoing investigations, or processed in the context of our anti-money laundering policy), for a minimum of 5 years, in accordance with applicable legislation and our internal money laundering process. This includes basic information data, KYC customer data, financial data, transaction data, and certain device, browser and app data. We keep this information regardless of your request to delete it,

if you have purchased Products that require KYC or if you have exhibit suspicious behaviour in your dealings with the Company. In some cases the Regulator (GIIF now, then Commission of Financial Supervision) may ask us to extend the retention time for certain data for another 5 years.

We will keep information that is relevant for tax purposes for up to 10 years.

7. MINORS

We understand the importance of protecting children's privacy, especially in an online environment. The Websites covered by this Privacy statement are not intentionally designed for or directed at children, and our Terms and conditions and Terms of use require all users to be above the age of majority in their local country. We adhere to laws regarding marketing to children. We never knowingly collect or maintain personal information about individuals under the age of 18.

If you have any concerns about our websites, would like to know if your child has accessed our services, or would like to remove your child's personal information from our servers (if such an account/wallet was created despite our efforts), please contact us at info@kbjpay.com.

We assure you that if we learn that a minor under the age of 18 has provided us with personal information, we will use our best efforts to delete the information promptly.

8. CROSS - BORDER TRANSFERS OF DATA

To enable our platform and services we might need to transfer and store your data outside the European Economic Area (EEA). It might also be processed by our staff or our business partners, or third-party service providers who are based outside the EEA. By giving us your personal data, you're agreeing to this. We ensure these transfers comply with applicable data protection rules unless the destination country has been officially deemed to provide adequate protection. We will always take all reasonable steps to ensure that your data is treated securely and in line with this Privacy Notice.

When that happens, we rely on adequacy decisions from the European Commission, whenever possible, and on the European Commission's Standard Contractual Clauses to enable the transfer of data to third countries. We also rely on exemptions provided by the GDPR, for example in order to share personal information when requested by law enforcement authorities, or to connect with our suppliers in order to fulfil your order.

9. MISCELLANEOUS

9.1. Complying with any requirement of law, regulations or a professional body of which we are a member.

As with any provider of such type of services, we are subject to legal, regulatory and professional obligations. We need to keep certain records to demonstrate that our services are provided in compliance with those obligations and those records may contain personal data.

9.2. Improving and developing our services.

Where agreed with our clients, we may use information that we receive in the course of providing services for other lawful purposes, including analysis to better understand a particular issue, industry or sector, to improve our business, service delivery and offerings and to develop new technologies and offerings. To the extent that the information we receive in the course of providing professional services contains personal data, we will de-identify the data prior to using the information for these purposes.

9.3. Websites.

This section describes how the Company handles personal information collected through the Websites and any other Company Websites that link to this privacy statement (collectively, "the Websites").

By using the Websites and providing personal information to us, you acknowledge you have read this privacy statement, and, to the extent your consent is necessary and valid under applicable law, you consent to the collection, use and disclosure of such personal information by the Company and any third party recipients in accordance with this privacy statement.

Some websites of our Portal/ the Website may have (might have in future) privacy statements that differ from this one and/or contain additional information as required under local law. Please refer to the privacy statements on the sites you visit in order to understand how they collect and process your data. By accessing any sites available within the Websites or content within them, you (a) acknowledge you will review those Privacy statements and (b) to the extent required under applicable law, consent to the collection, processing and use of your personal data as described in those Privacy statements.

We do not intend to collect sensitive information through the Websites unless we are legally required to do so. Examples of sensitive information include race or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; physical or mental health; genetic data; biometric data; sexual life or sexual orientation; and criminal records. We ask that you do not provide sensitive information of this nature when using the Websites. If you choose to provide sensitive information to us for any reason, the act of doing so constitutes your explicit consent, where such consent is necessary and valid under your local law, for us to collect and use that information in the ways described in this section of this Privacy statement or as described at the point where you choose to disclose this information.

We also do not actively seek demographic information from visitors to the Websites. However, you may choose to provide such information (including for example when becoming a Registered User, visiting our site from a social media site, submitting a resume, or responding to an online job application). If you choose to provide demographic information to us, the act of doing so constitutes your explicit consent, where such consent is necessary and valid under applicable law, for us to collect and use that information in the ways described in this section of the Privacy statement or as described at the point where you choose to disclose this information.

It is our policy to collect only minimum personal information required. If the Websites seek non-mandatory personal information about you, you will be notified of this at the point of collection. If you believe a Website has collected excessive information about you, please contact us at info@kbjpay.com to raise any concerns.

Some pages on the Websites may permit you to send emails to us. Messages sent via the Websites will contain your screen name and email address, as well as any additional information you wish to include in the message.

9.4. Third Party Links.

The Websites may link to third-party sites not controlled by the Company and which do not operate under the Company' privacy practices. When you link to third-party sites, the Company' privacy practices no longer apply. We encourage you to review each third-party site's privacy policy before disclosing any personally identifiable information.

9.5. Marketing

Where we are legally required to obtain your explicit consent to provide you with marketing materials, we will only provide you with such marketing materials if you have provided consent for us to do so.

If you opt into any subscriptions, you will receive automated emails when content is updated. If you opt into any newsletters, you will receive curated emails known as newsletters.

9.6. Unsubscribe

If you want to unsubscribe from mailing lists or any registrations, you should look for and follow the instructions we have provided within the appropriate area(s) of the Websites or in the relevant communications to you.

If you do not wish to receive emails or marketing communications from us, you can at any time contact us to request that such communications cease. If you wish to unsubscribe or no longer receive only certain communications, please identify such communications in your request.

If you choose to unsubscribe from any or all mailings, we may retain information sufficient to identify you so that we can honour your request.

9.7. Account Deactivation

If you are a Registered User, you may deactivate your account/ wallet at any time via the Registered User section of the Websites. If you deactivate your account/ wallet on the Websites, you will no longer receive the benefits of being a Registered User. If you choose to deactivate your account/ wallet, we may retain information sufficient to identify you so that we can honour your request.

If you have other registrations with Company, or have provided your information to the Company through other means (such as subscribing to newsletter), those registrations will be maintained unless you take specific action to inform us to cease contacting you.

Any user generated content that you may have created before then will not be anonymised following deactivation, nor will it be immediately removed from our systems or records.

10. COOKIES.

10.1 What are "cookies"?

Cookies are very small pieces of data, stored in text files on your computer or other device when websites are loaded in a browser. They are used mainly to "remember" you and your preferences. In many sites, they ensure a consistent and efficient experience for visitors, and perform essential functions such as allowing users to register and remain logged in. Cookies can be set by the site that you are visiting (known as "first party cookies"), or by third parties, such as those who serve content or provide advertising or analytics services on the website ("third party cookies"). Websites may also contain other similar technologies such as "web beacons" or "pixels." These are typically small transparent images that provide us with statistics, for similar purposes as cookies. They are often used in conjunction with cookies, though they are not stored on your computer in the same way. As a result, if you disable cookies, web beacons may still load, but their functionality will be restricted. For the purposes of this policy, we will use "cookies" as also including "web beacons" or "pixels".

10.2 How can you control the use of cookies in this website?

A "cookie notice" appeared when you accessed our website, requesting your consent for the use of cookies. Your consent should be free, explicit, unambiguous and properly informed by this Cookie Policy. When you consent in this manner, we place advertising cookies on your browser. If you do not provide consent, we will not deploy any cookies in your browser. By doing so, you won't share information with our analytics tool about events or actions that happen after the opt-out.

10.3 Registered users

We use these technologies to make navigation of the Websites easier for you and to better deliver tailored content to you. If you choose to become a Registered User: (a) we will use cookies to facilitate your registration and remember your preferences, (b) you will receive the benefits

of registration only if you accept the strictly necessary cookies, which include those cookies used as part of registration.

10.4 Analytics and site statistics

We also use these technologies to gather usage information and statistics regarding use of the Websites. For example, we collect information about page visits and navigation to determine what content is of greatest interest and if users are able to find content easily. Likewise, we collect information about which content is viewed and whether content is viewed in their entirety to determine what content is of most interest to users. We also use usage information to generate various reports regarding use of the Websites. These reports contain aggregated information about users and do not single out users individually. If you are a Registered User we may also collect information on what specific interests you have in order to understand what content interests you most. Information about the cookies used on our Websites can be found below.

10.5 Measuring effectiveness of our activities

We may utilise online identification technologies from marketing partners, third party sites and social media platforms. These technologies help us measure the efficacy of our marketing and awareness campaigns and to understand how visitors navigate to the Websites from Partners ad. We use these technologies to compile statistics about visitors who interact with the Websites online content, to gauge the effectiveness of our ads, and to provide more pertinent information to our visitors.

10.6 Managing cookies on your device

You can control and manage cookies using your browser. Please note that removing or blocking cookies can impact your user experience and some functionality may no longer be available.

Remember, cookies are there to improve your experience on our site.

10.7 Using your browser to control cookies

Most browsers allow you to view, manage, delete and block cookies for a website. Be aware that if you delete all cookies then any preferences you have set will be lost, including the ability to opt-out from cookies as this function itself requires placement of an opt out cookie on your device.

10.8 Managing Analytics cookies

You can opt-out of having your anonymised browsing history within our websites or applications recorded by analytics cookies.

10.9 Cookie disclosure

The following section explains the types, categories and purpose of cookies on the Websites. By using these Websites you consent to the deployment of cookies for the stated purpose.

10.9.1 Types of cookies:

(1) Session cookies: these cookies remain in your browser during your browser session only, i.e. until you leave the website.

(2) Persistent cookies: these cookies remain in your browser for a set period of time after the browser session (unless deleted by you).

10.9.2 Categories of cookies:

(1) Strictly Necessary Cookies: These cookies are fundamental to website functionality and cannot be switched off without blocking features on the site. They are usually set in response to your actions on the site, such as filling in forms, setting preferences, or logging in.

(2) Analytical Cookies: These cookies allow us to gather analytics to improve the performance and functionality of our site. These analytics can include measurements on the popularity of a page, common patterns of how people browse around the site, and how frequently a certain feature is used. We usually aggregate the data for review but in some cases we may collect information on content you have viewed in order to understand what interests you most.

(3) Customization cookies: These cookies help us to understand how effective our marketing campaigns are, and enhance your online experiences with us with customization.

(4) Advertising cookies: Company may present ads to you on sites that are not owned or operated by Company to promote Company services, articles or events. The cookies are used to make advertising messages more relevant to you and your interests. They also perform functions like preventing the same ad from continuously re-appearing. These advertisements are solely intended to make you aware of relevant Company promotions. Company does not sell your data to any third parties.

Please see above for more details.

11. COMPLAIANT SUBMISSION PROCESS

11.1 Under the General Data Protection Regulation (GDPR), which is a comprehensive data protection law in the European Union (EU), organizations are required to have a clear and transparent complaint policy related to privacy data. This policy ensures that individuals have avenues to raise concerns or complaints regarding the handling of their personal data by organizations.

11.2 Complaint Submission Process.

11.2.1 The Company's Complaint Channel - complaints related to GDPR compliance may be submitted to Company info@kbjpay.com.

11.2.2 Submission of Complaint - You submit your complaint through the above mentioned e-mail. The complaint should include sufficient details to allow Company to understand the nature of the concern, including relevant

information such as the your contact details, the specific data processing activities in question, and the alleged GDPR violations.

11.2.3 Acknowledgment of Receipt - Upon receiving a complaint, Company promptly acknowledges you the receipt of the complaint. This acknowledgment serves to reassure you that your complaint has been received and is being taken seriously. It includes an indication of the expected timeframe for further communication or resolution.

11.2.4 Initial Assessment - Company conducts an initial assessment of the complaint to determine its validity and seriousness. This involves reviewing the information provided by you, assessing whether the complaint falls within the scope of GDPR, and identifying any immediate actions that are necessary to mitigate risks or address concerns.

11.2.5 Investigation and Resolution - If your complaint is deemed credible and falls within the Company's responsibility under GDPR, an investigation is initiated. This investigation involves gathering additional information, interviewing relevant parties, reviewing relevant documentation, and assessing compliance with GDPR requirements. Based on the findings of the investigation, the Company takes appropriate actions to address the complaint, which includes implementing corrective measures, providing remedies to affected individuals, or making changes to its data processing practices.

11.2.6 Communication with Complainant - Throughout the process, the Company maintains communication with you to provide updates on the status of the investigation and any actions taken to address the complaint. This communication helps to keep you informed and engaged, demonstrating transparency and accountability.

11.2.7 Resolution and Follow-Up - Once the complaint has been adequately addressed and resolved to the satisfaction of both parties, the Company communicates the outcome to you. This communication includes details of the actions taken and any remedies provided.

11.2.8 Documentation and Record-Keeping - Throughout the complaint handling process, the Company maintains comprehensive records documenting the details of the complaint, the investigation process, and the actions taken to resolve it. These records serve as evidence of GDPR compliance and may be subject to regulatory scrutiny.

11.3 Escalation and External Remedies - If you are not satisfied with the Company's response to your complaint, you have the right to escalate the matter internally within the Company (by using appeal from first decision) or seek external remedies through Polish data protection authorities.

11.4 Polish data protection authority - The President of the Office for Personal Data Protection. Office of the President for Personal Data Protection [Urzad Ochrony Danych Osobowych], Stawki 2 Str. 00-193 Warsaw. Poland.

11.5 More information you can find at: https://gdpr.eu/what-is-gdpr/

11.6 To contact your local GDPR Authority within EU please see the website: https://www.edpb.europa.eu/about-edpb/about-edpb/members_en#member-pl

11.7 To find non-EU GDPR Authority please navigate through your local GDPR resources.

12. LEGAL DISCLAIMER

The information contained in this document is for general guidance on matters of interest only.

The application and impact of laws can vary widely based on the specific facts involved.

Given the changing nature of laws, rules and regulations, and the inherent hazards of electronic communication, there may be delays, omissions or inaccuracies in information contained in Websites. While we have made every attempt to ensure that the information contained in this site has been obtained from reliable sources, Company is not responsible for any errors or omissions, or for the results obtained from the use of this information.

All information in this site is provided “as is”, with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose.

In no event will Company, its related member entities, or the partners, agents or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information in this Site or for any consequential, special or similar damages, even if advised of the possibility of such damages.

This Global Privacy Policy (GDPR) was created on 08/01/2024 and is effective from that date. Any changes will be published accordingly. Each customer will be notified of the changes via the standard communication channels.