# General Privacy Policy BackB Investments S.à r.l.

**Effective Date**: 06.05.2024

**BackB Investments S.à r.l.** ("we", "us", or "our") is committed to protecting the privacy and security of your personal data, as well as your rights and freedoms of data subjects, according to the European General Data Protection Regulation (GDPR). The core principles of personal data processing: lawfulness, transparency, purpose limitation, data minimization, accuracy, storage limitation, confidentiality, integrity, and accountability, underlie our business activities. This Privacy Policy explains how we collect, use, disclose, and protect the personal data we gather through our website, while providing our services and during daily business.

| | |
|---|---|
| **Data Controller** | **BackB Investments S.à r.l. (the "BBI")** is a financial holding company, part of B2 Impact Group, offering solutions to the challenges created by defaulted loans. Through transparent and ethical debt management we build financial health. |
| **Contact Details** | **Head Office:** 9, rue Joseph Junck, L-1839 Luxembourg<br>**Email:** dpo@b2upi.com<br>**Website:** www.b2-impact.com/about-us/luxembourg/backb |
| **Contact Us** | If you have any questions, concerns, comments, or requests regarding this Privacy Policy or our data practices, please contact us to dpo@b2upi.com |

## Privacy policy – Main chapters:

1. Website users' privacy policy ..... 2
2. Email exchange privacy policy ..... 7
3. Business partners privacy policy ..... 11
4. Job candidates ..... 19
5. Who we share your data with? ..... 21
6. International data transfers ..... 22
7. How do we protect your data? ..... 22
8. Your rights ..... 23
9. Privacy policy updates ..... 24
10. Key legal and technical terms used in the privacy policy ..... 24

# 1. Website users' privacy policy

**This Privacy Policy applies to our website users.**

**Content of the Website Users Privacy Policy**

1.1. What Information Do We Collect and How?
1.2. Why We Use Your Information and How We Do It Legally?
1.3. Third-Party Services and Tools
1.4. How Long Do We Keep Your Data?
1.5. Automated Decision and Profiling.

## 1.1 Website users – What information do we collect and how?

This Website collects some Personal Data from its Users. Users are responsible for any third-party Personal Data obtained, published, or shared through this Website and confirm that they have the third party's consent to provide the Data to us.

**Data Collection**

When you visit and use our website, we collect certain data to enhance your experience and provide you with the right content.

The data collection methods we use may include:

- **Voluntary Information -** Data you share with us when you interact with our site, and you choose to share some personal info by filling out forms, subscribing to our newsletters, or engaging with our content.
- **Automatic Information**: We collect data automatically during your visit, such as your IP address, browser type, device information, and website usage patterns. This data is obtained through cookies and similar technologies.

**Categories of Personal Data Processed** when you visit our website may include the following types of data, collected by ourselves or through third parties:

| | |
|---|---|
| **Technical Information** | We may collect technical details about your device, browser, and internet connection when you access our website. |
| **How You Use Our Site** | We keep track of what you do on our site, like which pages you visit, what links you click, and other actions. This helps us improve the site and personalize your experience. |
| **Cookies Data** | We use cookies and similar technologies to collect info like your IP address, browser type, and how you browse. Cookies enable us to customize your experience, remember your preferences, and track website usage for analytical purposes. |
| **Contact Information and Subscription Data** | If you choose to contact us through our website or if you sign up for newsletters or updates, we may collect your name, email address, phone number, city, company name, and any other information you provide in your communication. We use this information to respond to your inquiries, provide support, and keep you in the loop for our latest news. You have the right to unsubscribe from these communications at any time. |
| **Opt-In Data** | When you visit our site, we might ask for your permission to use non-essential cookies, which are small text files placed on your device. These cookies help us improve our site and offer a personalized experience. You have the choice to accept or decline these cookies. Your preferences are stored, so we know whether to use them or not when you visit our site. You can adjust your cookie settings at any time through your device or browser settings. Please note that some cookies, like those needed for site security, will remain active. |

| | |
|---|---|
| **Demographic Information** | If you choose to provide it, we might collect info about your age, gender, location, or preferences. |
| **Geographic Position** | We may collect your approximate location (like your country and city) with your permission. This helps us provide location-based services and enhance your site experience. Please note that we collect this data with your consent, which you can withdraw at any time through your device or browser settings. |
| **Other necessary data** | Depending on your interactions, we might process additional personal data, such as identification information, user-generated content, usage data, contact details, incident reports, and more. |

When you are visiting our website, we don't collect financial info, social security numbers, or sensitive personal data through our site. We only gather what's needed for the purposes we've explained in our Privacy Policy. We process your data with your consent, for our legitimate interests in improving our site and services, and to meet legal obligations.

**Obligation to Provide Personal Data**
Website Users are not obligated to provide personal data. Data collection is primarily based on voluntary sharing and consent. Additionally, some data, such as technical information related to essential cookies, may be automatically collected during website visits to ensure security.

Users can still access and use many features of the website without providing personal data. However, choosing not to share certain data may limit the extent to which the website can offer a personalized experience. Users may receive more generic content and may not benefit from tailored recommendations.

## 1.2 Website users – Why we use your information and how we do it legally

We process your personal data collected through our website for the following purposes, as described below, and rely on different legal grounds for such processing, as permitted by applicable data protection laws.

Please note that we do not provide online services directly through our website, and we do not engage in automated decision-making or profiling activities that significantly affect you based on the data collected through our website.

| Purpose | Details on the Purpose | Legal Base | Data Processed |
|---|---|---|---|
| **Website Security** | We process your personal data to protect our website's security, prevent unauthorized access, and stop fraudulent activities. | Legitimate Interest | IP addresses, device information, browser information, website usage data, clickstream data, and session info. |
| **Responding to Inquiries**<br>**Contact Form**<br>**Phone Contact** | When you contact us through our website, we process your data to respond to your inquiries or support requests. | Legitimate Interest | Contact info (e.g., name, email, phone), user-submitted inquiries or support requests. |
| **Cookie Consent Recording** | We request and record your consent for non-essential cookies and manage cookie preferences to comply with legal requirements. | Legal Obligation<br>Legitimate Interest | Recording of your consent for non-essential cookies, cookie preferences, device and browser info, IP address. |

| | | | |
|---|---|---|---|
| **Data Retention Execution** | We process data to meet legal obligations, like record-keeping requirements, data retention and erasure requirements | Legal Obligation | Erasure of data collected after retention period has expired. |
| **Responding to Legal Requests** | We process data to respond to legal requests, such as court orders or law enforcement inquiries. | Legal Obligation | All personal data collected through our website |
| **Website Analytics and Performance** | We use data for website analysis to enhance performance and user experience. | Legitimate Interest | Website usage data, clickstream data, session info, device info, browser info, anonymized data, preferences. |
| **Research and Development** | We process data to improve website features | Consent | Website usage data, user feedback, survey responses |
| **Newsletter Subscription and Mailing List** | With your consent, we send news about our services, or upcoming events | Consent | Contact info (e.g., name, email), city, company, usage data |
| **Location-based Interactions** | We collect geolocation data with your consent to enhance your website experience. | Consent | Geographic Position |
| **Customizing User Experience** | We personalize your website experience based on your preferences. | Consent | Website usage data, page views, clickstream data, session info, device info, browser info. |
| **User Feedback and Surveys** | We gather user insights through feedback and surveys to improve our services. | Consent | User-provided feedback, survey responses, and any shared personal data. |
| **Cookies and Tracking Technologies** | We collect data about your browsing activities, preferences, and interactions through cookies and similar technologies. | Consent (Unless strictly necessary) | Cookies, IP address, device information, browser information, website usage data. |
| **Personalized Marketing and Advertising** | We collect data to deliver personalized marketing communications and targeted advertising based on your website preferences and behavior. | Consent | Cookies, IP address, device information, browser information, website usage data, demographic information, visitor interactions. |
| **Monitoring and auditing** | Monitoring and auditing purposes, such as internal or external audits, compliance assessments, adherence to security standards. | Legitimate interest | Identifying info, documentation, audit logs, records, compliance data. |

## 1.3 Website users – Third-party services and tools

Based on your consent and provided preferences, we use statistical and marketing cookies from Matomo Analytics and Google Analytics to enhance our website functionality, analyze user behavior, and improve our services.

These cookies help us understand how our website is used and provide you with tailored content and marketing communication.

In simple terms:

- **Statistical Cookies (First Party)** come from our website directly. These cookies track your website usage and help us improve our site. Data collected includes page visits and duration, typically retained for up to 12 months.

- **Marketing Cookies (First Party)** also come from our website. These cookies understand your interests based on your site interactions, allowing us to show relevant ads. Data collected includes website interactions and is typically retained for up to 12 months.

Our trusted partners assist us in managing these cookies.

- **Matomo Analytics** is an open-source web analytics platform, to collect and analyze data about our website's usage.

  For more information about Matomo Analytics' privacy practices, please review Matomo's Privacy Policy on their website: Privacy Policy - Analytics Platform - Matomo

  Matomo Analytics is provided by InnoCraft Ltd, located in New Zealand while 100% of the data collected and backups are securely stored in Europe. Although New Zealand is outside Europe Economic Area ("EEA"), is one of the countries that the EU considers to have an adequate level of data protection.

- **Google Analytics** and its related products is a web service provided by Google Ireland Limited ("Google") for users of Google services based in the European Economic Area.

  For more information about Google Analytics' privacy practices, please review Google's Privacy Policy on the Google website: Privacy Policy – Privacy & Terms – Google.

  When using Google Analytics for users located in the European Economic Area (EEA), the data collected is typically stored within the European Union (EU) or the European Economic Area. By way of exception data may be stored in servers located in USA.

For detailed information about these cookies and data handling, please check our **Cookie Policy** Cookie Policy (b2-impact.com). Your privacy is important, and we want you to make informed choices while using our website.

## 1.4 Website users – How long do we keep your data?

We keep your data as long as we need to for legal reasons or as long as necessary to fulfill the purposes outlined in this Privacy Policy.

The time we keep it might change based on things like:

- Type of Data - Some data needs longer keeping than others.
- The purposes for which we process your personal data.
- Legal and regulatory requirements. Sometimes the law says we must keep data.
- Our business needs and operational requirements affect how long we keep data.

We may be required to retain certain personal data for a longer period to comply with legal and regulatory obligations, resolve disputes, and enforce our rights.

During the retention period, we will take appropriate technical and organizational measures to ensure the security and confidentiality of your personal data. Once the retention period expires, we will securely delete or anonymize your personal data in accordance with applicable laws and regulations.

| | |
|---|---|
| **Technical Information** | Up to 12 months |
| **Website Usage Data** | Up to 12 months |
| **Cookies Data** | Usually until you finish browsing, or up to 12 months |
| **Contact Information** | For 3 years, so we can respond and document your requests. |
| **Opt-In Data** | Until you unsubscribe or ask us to remove it. |

| | |
|---|---|
| **Demographic Data** | Up to 12 months if you provide it. |
| **Geographic Position** | Up to 12 months, and you can change your settings anytime. |
| **Other Necessary Data** | Up to 3 years, depending on what data is and why we collected it. |

Remember, you have rights about your data, like asking us to delete it in certain situations. To know more about your rights and how to use them, check our "Your Rights" section in the Privacy Policy.

## 1.5 Website users – Automated decision and profiling

**Automated Decision-Making:** We do not engage in automated decision-making processes that produce significant legal effects or similarly significant consequences for individuals based solely on automated processing.

**Profiling:** We may use profiling techniques in the following contexts:

- **Personalization of User Experience** to customize your website experience based on your preferences and past interactions. This allows us to provide you with content and features that are most relevant to you**.**
- **Personalized Marketing Communication** involves analysing your data to deliver targeted ads and marketing messages that align with your interests and behaviour.
- **Website Analytics and Performance** to track user behavior, such as page views and clickstream data, to understand how users interact with the site. This data is used to improve website performance, enhance user experience, and optimize content placement.
- **Cookies and Tracking Technologies** are used to collect data on user behavior, preferences, and interactions with our website. This data is valuable for understanding user preferences, providing personalized experiences, and improving website functionality.
- **Security Profiling** based on monitoring and auditing involves tracking user activities, access logs, and compliance data to ensure adherence to security standards and regulations. This is done to maintain the security and integrity of the website, protect against unauthorized access, and demonstrate compliance with legal requirements.

In summary, the profiling activities described above are implemented with the intention of enhancing your user experience and improving website performance. We value your privacy and offer options for consent and control over your data preferences. If you have any questions or concerns about our profiling practices, please don't hesitate to contact us using the information provided in our "Contact Us" section.

# 2. Email exchange privacy policy

**This Privacy Policy applies to all individuals involved in email exchange communication with us, including:**

- Customers (Debtors)
- Clients and Potential clients
- Investors
- Business partners, suppliers, and external advisors
- Employees
- Candidates
- Legal Authorities
- Other stakeholders involved in the email exchange process.

**Content of the Email Exchange Privacy Policy**

2.1 What Information Do We Collect and How?

2.2 Why We Use Your Information and How We Do It Legally?

2.3 Third-Party Services and Tools

2.4 How Long Do We Keep Your Data?

2.5 Automated Decision and Profiling

## 2.1 Email exchange – What information do we collect and how?

**How is data collected?**

We collect personal data through various means to facilitate our email exchange process and ensure security.

If you choose to share information about other individuals, please bear in mind that you are responsible for any third-party Personal Data obtained and shared through the email exchange process and you confirm the third party's consent to provide such Data to us.

- **Direct Collection** includes information you provide like data directly shared by you during email exchanges, such as your name, contact details, professional information, and the content of emails, including text and attachments.
- **Indirect Collection from Publicly Available Sources.** We may collect publicly available information about you from sources like professional social media profiles, business websites, or public directories, if such information is relevant to our email exchange process.

**What categories of data are processed?**

The specific personal data collected may vary depending on the nature of our email exchanges and the purposes for which they are conducted. We ensure that all data, including sensitive data, is processed in accordance with applicable data protection laws and for the purposes outlined in this Privacy Policy.

During our email exchange process, we may process the following categories of data:

| | |
|---|---|
| **Identification Information** | Your name, contact details (like phone and mailing addresses), and any other personal information shared during email exchanges, like employee IDs, and usernames. |
| **Professional Information** | Job titles, company names, industry affiliations, professional qualifications, and business contact information. |

| | |
|---|---|
| **Communication Data** | The content of emails exchanged, including text, attachments, documents, images, and any other information shared during our correspondence. |
| **Sensitive Data** (Only if provided by you) | By exception, if you voluntarily choose to share sensitive data with us during email exchanges. Sensitive data may include any personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation health-related information, or other data classified as sensitive under applicable data protection laws. Any sensitive data shared with us will be processed in accordance with the highest standards of data protection and only for the specific purposes for which it is provided by you. |
| **Communication Metadata Logs and IT Usage Data** | To investigate and document incidents, check phishing emails, and maintain security, we may collect logs and other IT usage data related to email communications. This data may include timestamps, email addresses, and subject lines related to our email communications, server logs, IP addresses, device information, email delivery logs, metadata related to email exchanges, and information for security monitoring and incident response. |
| **Financial and Transaction Data** (if relevant) | Billing information, financial transaction records, payment details, bank account and invoices related to professional agreements, order histories, and details of products or services discussed during email exchanges. |
| **Other necessary data** | Depending on your interactions, we might process additional personal data, such as information related to our professional agreements, project details, event information, or contractual terms and any other data relevant to our professional relationship. |

Please note that the specific data categories processed during email exchanges may vary depending on the nature of the professional interaction and the information you choose to share with us via email exchange. We are committed to handling all data with care and in accordance with applicable privacy laws and regulations.

**Obligation to Provide Personal Data during Email Exchange**
In the context of email exchange, usually the communication is initiated by you, while providing your personal data voluntarily through the email correspondence. Users are not obligated to provide such personal data for email exchange. However, the absence of certain data may impact the effectiveness of email communication and limit our ability to address your inquiries or provide specific information.

## 2.2 Email exchange – Why we use your information and how we do it legally

In this section, we outline the specific purposes for which we collect and process your personal data during the email exchange process, along with the legal bases and categories of data processed for each purpose.

| Purpose | Details on the Purpose | Legal Base |
|---|---|---|
| **Facilitating Email Communication** | We process your personal data to facilitate email communication and correspondence between you and our organization. | Contract execution or taking steps to enter a contract and/or Legitimate interest to communicate with you efficiently and effectively through email for business-related matters. |
| **Compliance with Legal Obligations** | We may process your personal data to comply with legal obligations, including record-keeping, regulatory requirements, and responding to legal requests. | Compliance with a legal obligation to which we are subject. |

| | | |
|---|---|---|
| **Responding to Inquiries** | We may process your personal data to respond to inquiries, questions, or requests made via email. | Contract execution or taking steps to enter a contract and/or Legitimate interest to communicate with you efficiently and effectively through email for business-related matters. |
| **Sending Newsletters and Updates** | If you have provided consent, we may use your email address to send newsletters, updates, or promotional materials related to our services or products. | Consent (you have the right to withdraw your consent at any time). |
| **Customizing User Experiences** | We may process data related to your email interactions to personalize and improve your user experience. | Legitimate interests in providing you with a better and more personalized experience. |
| **Research and Development Business Analytics and Reporting** | We may use aggregated email data for business analytics, reporting, and performance assessment, for research and development purposes to enhance our services and activity. | Legitimate interests in monitoring and improving our business operations |
| **Fraud Prevention Incident Investigations Security Monitoring** | We may process email, IT usage data and logs to prevent fraudulent activities, unauthorized access, check phishing emails, ensure security monitoring and to investigate and document security breaches, data breaches, or other incidents that may affect the security of your personal data. | Legal obligations to investigate and document incidents and Legitimate interests in protecting our business from fraud and maintaining the security of email communications. |
| **Dispute Resolution** | In the event of disputes arising from email exchanges, we may process relevant personal data to facilitate resolution, investigations, or legal proceedings. | Legitimate interests related to the establishment, exercise, or defence of legal claims. |
| **Complaints Resolution Handling Data Subjects Requests** | To address and resolve complaints or concerns raised by you or third parties regarding our services, processes, or treatment of personal data and to respond to data subjects' requests. | Legal obligations to document and respond complaints and data subjects' requests, and/or Legitimate interests related to the establishment, exercise, or defence of legal claims. |
| **Improving Services Business Development** | We may process email data to monitor the quality of our services, identify areas for improvement, enhance the overall user experience, identify potential business opportunities, collaborations, or partnerships. | Legitimate interests in maintaining and improving our services and pursuing business growth and development. |
| **Internal Audit External Audit Compliance Monitoring** | To conduct internal and external audits and ongoing compliance monitoring to ensure that our organization adheres to regulatory requirements, policies, and internal standards. | Legal Obligation and/or Legitimate Interests |
| **Risk Management and Control Activities** | To assess, manage, and control risks related to data security, privacy, and compliance. | Legitimate Interests in ensuring risk management, sustainability, and compliance of our operations. |
| **Sensitive Data Processing** | To process sensitive data voluntarily provided by you during email exchanges for specific purposes as agreed upon. | Consent and/or Legitimate interests related to the establishment, exercise, or defence of legal claims. |

Please note that the specific purposes and legal bases for processing may vary depending on the circumstances and your interactions with us. We always ensure that personal data is processed in accordance with applicable data protection laws and with respect for your privacy rights.

It's important to emphasize that when processing personal data for legitimate interests, we balance these interests with the rights and freedoms of the individuals whose data is being processed. We take measures to ensure your rights are respected, and that personal data is processed in a fair and lawful manner.

## 2.3 Email exchange – Third-party services and tools

We may utilize various third-party tools and services to optimize our email exchange process, ensuring efficient communication and security. These tools may have access to email content or metadata to provide their services. We carefully select and work with trusted third-party providers who comply with data protection standards and confidentiality requirements. Please note that our use of third-party tools is always aimed at enhancing the quality and security of our email exchanges.

## 2.4 Email exchange – How long do we keep your data?

We retain your data as long as needed for email communication and mainly up to 3 years after the end of the email exchange for legal and dispute resolution purposes.

However, please be aware that in certain cases, depending on the subject and content of the email correspondence, the retention period may be longer according to the specific purposes and regulatory requirements.

For example, if we have a contractual relationship, we may retain relevant data for up to 5 years after the contractual relationship is closed or if other legal deadlines apply.

We always ensure compliance with relevant legal obligations and adjust our retention periods accordingly to meet these requirements. Our primary goal is to maintain data for as long as necessary to fulfil the purposes outlined in this Privacy Policy and to meet any legal obligations.

During the retention period, we will take appropriate technical and organizational measures to ensure the security and confidentiality of your personal data. Once the retention period expires, we will securely delete or anonymize your personal data in accordance with applicable laws and regulations.

Remember, you have rights about your data, like asking us to delete it in certain situations. To know more about your rights and how to use them, check our "Your Rights" section in the Privacy Policy.

## 2.5 Email exchange – Automated decision and profiling

We emphasize that our email exchange data processing activities do not involve automated decision-making that significantly affects individuals. Our primary focus is on data collection for email communication, security, and analytics, and we do not engage in any automated decision-making processes that could impact your rights and freedoms.

Profiling Activities in Email Exchange process may be used only in the context of **Security Risk Profiling**:

- We perform automated processing of email usage and related technical data from IT systems, such as access logs, IP addresses, and device data, to identify potential security threats and vulnerabilities, unauthorized access, phishing attempts, and other security risks.
- This profiling activity is important to safeguard the security of our email exchange process, IT infrastructure and environment.

- The processing helps us proactively respond to security incidents, investigate security breaches, and maintain the confidentiality and integrity of email communications.

The logic is to provide a safer, more transparent, and efficient environment to engage in professional relationships. The significance lies in improved security. The envisaged consequences are generally positive and aim to enhance the overall experience and outcomes for our communication.

Please be assured that any profiling activities are conducted in compliance with relevant data protection laws and regulations. You have the right to object to profiling processes, where appropriate.

If you have any concerns or questions about automated decision-making or profiling in our company, please do not hesitate to contact us using the contact details provided in the "**Contact Us**" section of this Privacy Policy.

# 3. Business partners privacy policy

**This Privacy Policy applies generally to all our existing and potential Business Partners including:**

- Clients
- Investors
- Vendors
- Suppliers
- External Advisors
- Any third party involved in a business relationship with Us.

**Content of the Business Partners' Privacy Policy**

3.1 What Information Do We Collect and How?

3.2 Why We Use Your Information and How We Do It Legally?

3.3 Specific Information regarding Due Diligence Process (Sanctions and PEP Screening)

3.4 Third-Party Services and Tools

3.5 How Long Do We Keep Your Data?

3.6 Automated Decision and Profiling

## 3.1 Business partners – What information we collect and how?

**How is data collected?**

We collect personal data through various means to facilitate our professional interactions and collaborations and ensure security.

If you choose to share information about other individuals, please bear in mind that you are responsible for any third-party Personal Data obtained and shared and you confirm the third party's consent to provide such Data to us.

- **Direct Collection** includes information you provide like data directly shared by you during business relationship and professional interactions, such as your name, contact details, professional information, and other relevant documents or information.

- **Indirect Collection from Publicly Available Sources.** We may collect publicly available information about you from sources like professional social media profiles, business websites, or public registers, if such information is relevant to our business relationship management.

**What categories of data are processed?**
During our professional interactions and collaborations, we may process a wide range of personal data necessary for the management and development of these relationships. The specific personal data collected may vary depending on the nature of our interactions and the purposes for which they are conducted. We are committed to handling all data with care and in accordance with applicable data protection laws and regulations.

Below are presented the main categories of personal data we may process:

| | |
|---|---|
| **Identification Information** | Name, contact details (like phone and mailing addresses), and any other identification information shared during business relationship and relevant for our cooperation. |
| **Professional and Business Information** | Job titles, company names, industry affiliations, professional qualifications, and business contact information. |
| **Communication Records** | Records of email correspondences, meeting minutes, call logs, and other communication-related data exchanged during our professional interactions. |
| **Legal Information** | Information resulting from legally binding documents, such as partnership agreements, contracts, and other relevant legal documents. |
| **Financial Information** | Billing information, financial transactions records, including bank account details, credit ratings, payment terms, financial transactions, billing history, invoices related to professional agreements, order histories, and details of products or services and other financial data relevant to our collaborations. |
| **Sanctions Screening Data** | Information about screening Business Partners against sanctions lists and databases of politically exposed persons, which may include sensitive data related to political opinions, criminal convictions, or fraudulent activities *(please check details in the next two sections).* |
| **KYC and AML Data** | Data resulting from Know Your Customer (KYC) and Anti-Money Laundering (AML) checks and assessments performed on Business Partners to detect and prevent money laundering activities. |
| **Conflict of Interest Data** | Data related to the assessment of potential conflicts of interest between our company and its Business Partners. |
| **Risk Assessment Data** | Information related to the risk assessment of Business Partners, considering factors such as financial stability, reputation, and compliance history. |
| **Regulatory Data** | Data related to regulatory requirements, certifications, licenses, permits, accreditations, and industry-specific qualifications obtained by our Business Partners. |
| **Intellectual Property Data** | Information about intellectual property rights and agreements between our company and its Business Partners, such as patents, trademarks, or copyrights. |
| **Performance Data** | Data related to the performance and service quality of our Business Partners, including service level agreements, performance evaluations, and feedback. |
| **Representatives' Data** | Data of employees or representatives of the Business Partners, such as names, job titles, contact details, and other relevant information for the business relationship management. |
| **Insurance Data** | Information about the insurance coverage and liability agreements between our company and the Business Partners. |
| **Marketing Preferences** | Preferences for marketing communications, feedback, survey results, and other marketing-related data shared during our interactions. |
| **Dispute Records** | Information related to any legal disputes or complaints that may arise during our collaborations. |

| | |
|---|---|
| **Audit and Compliance Data** | Data related to audits, assessments, or inspections conducted by / or related to the Business Partners to ensure compliance and quality. |
| **Access Rights and Permissions Data** | Data about the access rights and permissions granted to our Business Partners for different systems, applications, and IT resources within our company. |
| **Technical Data** | Technical information, such as system and application access logs, IP addresses, and the usage of corporate digital resources relevant to our collaborations. |
| **IT Data** | Information about the hardware and software used by Business Partners on their workstations, relevant for IT support purposes. |
| **Device Data** | Data about the devices used by Business Partners to access our IT systems, cloud environments, applications, or our IT infrastructure, such as laptops, smartphones, or tablets. |
| **Metadata Logs and IT Usage Data** | We may gather metadata logs and information related to IT usage across various systems and applications. This data plays important role in investigating and documenting incidents, verifying the authenticity of communications, and maintaining security measures. It may encompass diverse elements, including timestamps, user identifiers, system activity records, access logs, IP addresses, device details, application usage logs, server logs, cloud environment data, and metadata associated with various interactions. Additionally, this information aids in security monitoring and responding to incidents across our IT infrastructure, including but not limited to email systems, cloud environments, and other software applications and platforms integral to our business operations. |
| **Other Relevant Data** | Depending on your interactions, we might process additional personal data, such as information related to our professional agreements, project details, event information, or contractual terms and any other data relevant to our professional relationship. |
| **Sensitive Data** | By exception, in the context of our relationships with our Business Partners, sensitive data is only processed in specific situations, which include Sanctions Screening process where we may collect, and process sensitive data related to criminal convictions, fraudulent activities, or politically exposed person (PEP) status (if such information is disclosed in the public official lists) as part of our sanctions screening procedures to ensure compliance with regulatory requirements and mitigate potential risks associated with individuals or entities. It's important to note that the processing of sensitive data is carried out with the utmost care and in strict compliance with applicable data protection laws. Our primary aim is to safeguard the rights and freedoms of individuals while fulfilling our legal obligations and maintaining the highest ethical standards in our professional relationships. |

### Obligation to Provide Personal Data for Our Business Relationship

We request certain personal data from our Business Partners to fulfil key purposes such as risk assessment, compliance checks, and collaborations. The consequence of not providing this required data may include limited collaboration opportunities and impact on our business relationship:

- Non-provision of necessary data may restrict access to specific services, projects, or collaborations.
- The absence of critical data may constrain our ability to initiate or continue our business partnership.

We value data accuracy and reliability, ensuring transparency and ethical standards in our collaborations. We encourage Business Partners to provide the required personal data to facilitate effective risk assessments and mutually beneficial collaborations.

## 3.2 Business partners – Why we use your information and how we do it legally

In this section, we outline the specific purposes for which we collect and process your personal data during the email exchange process, along with the legal bases and categories of data processed for each purpose.

| Purpose | Details on the Purpose | Legal Base |
|---|---|---|
| **Managing Business Relationships** | Establish and maintain business relationships with our Business Partners, including communication, collaboration, and contractual arrangements. | Contract Execution or steps before entering into a contract.<br>Legitimate interests to have efficient business operations and collaboration. |
| **Billing and Payments** | Process financial transactions, billing, payments, and related financial activities necessary for our collaborations. | Contract Execution<br>Tax and Accounting Legal Obligations |
| **Facilitating Communication** | Facilitate communication through various channels and correspondence between you and our organization. | Contract execution or taking steps to enter a contract and/or<br>Legitimate interest to communicate with you for business-related matters. |
| **Responding to Your Inquiries** | We may process your personal data to respond to your inquiries, questions, or requests. | Contract execution or taking steps to enter a contract |
| **Sending Newsletters and Updates** | If you have provided consent, we may use your email address to send newsletters, updates, or promotional materials related to our services or products. | Consent<br>(You have the right to withdraw it at any time). |
| **Compliance with Legal Obligations** | We may process your personal data to comply with legal obligations, including record-keeping, regulatory requirements, and responding to legal requests. | Legal obligation |
| **Sanctions Screening and Risk Assessment** | We may process your personal data to screen Business Partners against sanctions lists and assess risks related to their financial stability, reputation, and compliance history. | Legal obligation<br>Legitimate Interest<br>*(Please check the details below in the next section)* |
| **Know Your Customer (KYC) and Anti-Money Laundering (AML)** | We may process your personal data to conduct due diligence and assessments on Business Partners to prevent money laundering and fraudulent activities. | Legal Obligation<br>Legitimate Interest to prevent fraud and illicit activities. |
| **Conflict of Interest Assessment** | To assess potential conflicts of interest between our company and its Business Partners to ensure transparency and ethical conduct. | Legitimate Interest in maintaining transparency and ethical conduct in professional collaborations |
| **Checking Regulatory Requirements** | To verify necessary certifications, licenses, permits, and industry-specific qualifications obtained by our Business Partners. | Legal Obligations related to regulatory requirements and certifications. |
| **Intellectual Property Rights Management** | To manage intellectual property rights and agreements between our company and its Business Partners, such as patents, trademarks, or copyrights. | Contract Execution<br>Legitimate interests related to the establishment, exercise, or defence of legal claims. |
| **Service Performance Evaluation** | To evaluate the performance and service quality of our Business Partners, including service level agreements and feedback. | Legitimate Interest in assessing and improving the quality of services provided by Business Partners. |

| | | |
|---|---|---|
| **Marketing and Surveys** | To manage marketing preferences, feedback, survey results, and other marketing-related data shared during our interactions. | Consent<br>(You have the right to withdraw it at any time). |
| **Dispute Resolution** | In the event of disputes arising from our cooperation, we may process relevant personal data to facilitate resolution, investigations, or legal proceedings. | Legitimate interests related to the establishment, exercise, or defence of legal claims |
| **Complaints Resolution Handling Data Subjects Requests** | To address and resolve complaints or concerns raised by you or third parties regarding our services, processes, or treatment of personal data and to respond to data subjects' requests. | Legal obligations to document and respond complaints and data subjects' requests.<br>Legitimate interests related to the establishment, exercise, or defence of legal claims. |
| **Fraud Prevention and Incident Investigations Security Monitoring** | We may process email, IT usage data and logs to prevent fraudulent activities, unauthorized access, ensure security monitoring and to investigate and document security breaches, data breaches, or other incidents that may affect the security of your personal data. | Legal obligations to investigate and document security incidents and<br>Legitimate interests in protecting our business from fraud and maintaining the security of email communications. |
| **Research and Development** | We may use aggregated data for research and development purposes to enhance our services and activity. | Legitimate interests in improving our offerings and activity |
| **Business Analytics and Reporting** | We may analyse data for business analytics, reporting, and performance assessment. | Legitimate interests in monitoring and improving our business operations |
| **Monitoring and Improving Services Business Development** | We may process data to monitor the quality of our services, identify areas for improvement, and enhance business or to identify potential business opportunities, collaborations, or partnerships. | Legitimate interests in maintaining and improving our services and pursuing business growth and development. |
| **Internal Audit External Audit Compliance Monitoring** | To conduct internal and external audits and ongoing compliance monitoring to ensure that our organization adheres to regulatory requirements, policies, and internal standards. | Legal Obligation and/or<br>Legitimate Interests |
| **Risk Management and Control Activities** | To assess, manage, and control risks related to data security, privacy, and compliance. | Legitimate Interests in ensuring risk management, sustainability, and compliance of our operations. |

Please note that the specific purposes and legal bases for processing may vary depending on the circumstances and your interactions with us. We always ensure that personal data is processed in accordance with applicable data protection laws and with respect for your privacy rights.

When processing personal data for our legitimate interests, we balance these interests with the rights and freedoms of the individuals whose data is being processed. We take measures to ensure your rights are respected, and that personal data is processed in a fair and lawful manner.

## 3.3 Business partners – Specific information on due diligence process (sanctions and pep screening)

### Purposes and Legal Grounds of the Screening

We perform screening process on Sanctions and Politically Exposed Persons (PEP) as part of our commitment to comply with applicable laws and regulations governing International Sanctions, Anti-Bribery and Anti-Corruption (ABC) measures, financial crime prevention, Know Your Customer (KYC) requirements, Anti-Money Laundering (AML) regulations, and Counter-Terrorism Financing (CTF) obligations. This screening

process is essential to identify and evaluate potential risks associated with individuals or entities involved in our business relationships or financial transactions.

The Sanctions & PEP screening serves several vital purposes, including:

- Ensuring compliance with legal obligations to avoid engaging in business relationships or financial transactions with persons or entities subject to international sanctions.
- Conducting due diligence and screening activities to prevent any misuse of our company for unlawful purposes.
- Facilitating effective risk management practices.
- Demonstrating our commitment to ethical and responsible business conduct.

We perform Sanctions and PEP screening process according to the General Data Protection Regulation ("GDPR") on the legal grounds provided by article 6(1) letters c) and f)[1], or by article 9(2) letter e) and f)[2].

These legal bases allow us to process your data (i) when necessary to comply with our legal obligations and (ii) when necessary for our legitimate interests, such as operating our business securely, protecting the integrity of our systems, operations, clients, business relationships, and users, detecting or preventing fraud, and fulfilling other legitimate interests.

## Collection of Personal Data, Categories of Data Subjects and Sources of Data

Our Sanctions and PEP screening process involves the collection and processing of personal data related to two key categories of data subjects:

- **Our Business Partners:** This category includes personal data such as full names, contact details, dates of birth, genders, nationalities, citizenships, countries of residence, client IDs, and other pertinent information. Additionally, business and financial data necessary for effective screening may be collected. We obtain this data directly from data subjects during our business relationships or indirectly from publicly available sources**.**
- **Individuals Included in Sanctions and PEP Lists:** This group comprises individuals listed on relevant Sanctions and PEP lists. The data processed for screening may include full names, dates of birth, genders, nationalities, citizenships, countries of residence, other identification information available in public official sources, contact details, functions or professions, details regarding sanctions, and other relevant publicly available information. We source this data from authorized databases, third-party screening providers, publicly accessible information, regulatory authorities, law enforcement agencies, international organizations, and commercially available PEP databases.

Please note that we have no control over the information contained in public official records and data sets collected by third-party screening providers. These data are gathered from various sources, and decisions regarding the disclosure of personal information rest with the relevant public bodies, balancing the public interest in disclosure and individuals' privacy rights.

## Screening Criteria and Possible Consequences in case of a Positive Match

[1] According to Article **6(1) letter c) and f) of GDPR**:" *Processing shall be lawful only if and to the extent that at least one of the following applies: (…) c) processing is necessary for compliance with a legal obligation to which the controller is subject*. (…); *f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (…)".*

[2] According to Article **9(2) letter e) and f) of GDPR**: "*(1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. (2) Paragraph 1 shall not apply if one of the following applies: (…) e) processing relates to personal data which are manifestly made public by the data subject; f) processing is necessary for the establishment, exercise, or defence of legal claims or whenever courts are acting in their judicial capacity. (…)"*

- **Screening Criteria**. During the screening process, we use advanced and secure technology and algorithms to compare personal data, such as names, dates of birth, nationalities, and other essential information, against relevant Sanctions and PEP lists. This process is automated but requires human intervention for further analysis and investigation in cases of positive matches. No automated individual decision-making is applied.
- **Consequences of a Positive Match.** If a positive match is detected during screening, it may trigger additional due diligence measures, such as enhanced monitoring or further investigation, as mandated by applicable laws and regulations. Our commitment is to handle such situations in full compliance with legal requirements while safeguarding the confidentiality and integrity of personal data.

### Data Retention

We retain personal data collected during the screening process only for as long as necessary to fulfill our legal obligations and legitimate business purposes.

- **Business Partners:** the data is actively processed during the business relationship and only stored for maximum 5 years[3], after the business agreement is closed.
- **Individuals on the Sanctions & PEP Lists from selected data sources:** the data is actively processed during each screening session and then automatically removed; the data resulting in potential matches is actively processed during the manual review and analysis and only stored for a period of maximum 5 years after the business relationship with the relevant business partner is closed.

### Data Sharing

In some cases, we may be required to disclose personal data to regulatory authorities, law enforcement agencies, or other authorized entities as part of our legal obligations or to fulfil our legitimate interests. We do not share personal data with any third parties for marketing purposes.

To know more about your rights regarding your personal data and how to use them, please check the relevant section "Your Rights" in this Privacy Policy.

## 3.4 Business partners – Third-party services and tools

While managing our business relationships with our partners, we may utilize various third-party tools and services to enhance our operations and facilitate effective collaboration. These tools and services are designed to streamline processes, improve communication, and support the secure exchange of information.

These third-party tools and services may encompass a variety of functionalities and solutions, enhancing our ability to work together efficiently and securely.

The use of these third-party tools and services may require the sharing of certain categories of personal data related to our Business Partners. The types of data shared may vary depending on the specific tool or service in use but can include information necessary for our professional collaborations.

We carefully select and work with trusted third-party providers who comply with data protection standards and confidentiality requirements. Please note that our use of third-party tools is always aimed at enhancing the quality and security of our activity and operations.

[3] Guide to the Money Laundering Act (part 2 – Section5.2. Registration and Storage of Information) issued by FINANSTILSYNET (Financial Supervisory Authority of Norway).

## 3.5 Business partners – How long do we keep your data?

We retain your data as long as needed for the execution and management of our contractual relationship and up to 5 years after the contractual relationship is closed or for longer period if other legal deadlines apply.

We always ensure compliance with relevant legal obligations and adjust our retention periods accordingly to meet these requirements. Our primary goal is to maintain data for as long as necessary to fulfil the purposes outlined in this Privacy Policy and to meet any legal obligations.

The time we keep it might change based on things like:

- Type of Data - Some data needs longer keeping than others.
- The purposes for which we process your personal data.
- Legal and regulatory requirements. Sometimes the law says we must keep data for specific periods.
- Our business needs and operational requirements affect how long we keep data.

During the retention period, we will take appropriate technical and organizational measures to ensure the security and confidentiality of your personal data. Once the retention period expires, we will securely delete or anonymize your personal data in accordance with applicable laws and regulations.

## 3.6 Business partners – Automated decision and profiling

**Automated Decision-Making:** We do not engage in automated decision-making processes that produce significant legal effects or similarly significant consequences for individuals based solely on automated processing.

**Profiling:** We may use profiling techniques in the following contexts:

- **Security Risk Profiling** involves analysing technical data from IT systems, such as access logs, IP addresses, and device data, to identify potential security threats and vulnerabilities. It is essential for ensuring the security of IT systems, tools, and applications during professional relationships. Due to this profiling, you can expect enhanced security measures to protect your data and the systems you interact with leading to a safer and more secure cooperation environment.
- **Risk Assessment and Due Diligence Profiling** techniques are employed to assess and manage risks related to Business Partners, covering financial stability, reputational issues, compliance history, certifications, licenses, permits, conflicts of interest, integrity due diligence, and fraud prevention. It helps in evaluating and managing compliance risks, integrity issues, and potential vulnerabilities within professional collaborations. In this way you can benefit from a more transparent and ethical business environment. The consequences include improved compliance, reduced fraud risks, and fairer partnerships.
- **Performance Profiling** techniques help us to assess the performance and service quality of our Business Partners by analysing performance metrics, service level agreements, and feedback data. It aids in evaluating and enhancing the efficiency and effectiveness of our cooperation. Consequences include better service quality and more efficient interactions tailored to meet both our needs.
- **Preferences Profiling** techniques analyse preferences expressed by you, including marketing communications, feedback, and various survey results. It enables tailored interactions and communications based on your specific preferences. In this way you can enjoy personalized and relevant interactions. Consequences include receiving communications and services that align with your preferences and interests.

In all profiling contexts, the logic is to provide a safer, more transparent, and efficient environment to engage in professional relationships. The significance lies in improved security, compliance, efficiency, and personalized interactions. The envisaged consequences are generally positive and aim to enhance the overall experience and outcomes for our business partnership.

Please be assured that any profiling activities are conducted in compliance with relevant data protection laws and regulations. You have the right to object to profiling processes, where appropriate.

If you have any concerns or questions about automated decision-making or profiling in our company, please do not hesitate to contact us using the contact details provided in the "**Contact Us**" section of this Privacy Policy.

# 4. Job candidates

This Privacy Policy applies to all Job Candidates and applicants who would like to apply for the job position in BackB Investments S.à r.l..

To ensure confidentiality and transparency of personal data processing and in accordance with honest information practices and applicable regulations on personal data protection, we would like to inform you that the controller of your personal data is BackB Investments S.à r.l. with its registered office at 9, rue Joseph Junck, L-1839 Luxembourg.

**Content of the Job Candidates' Privacy Policy**

4.1 What Information Do We Collect and How?

4.2 Why We Use Your Information and How We Do It Legally?

4.3 Who Are the Recipients Of Your Data

4.4 How Long Do We Keep Your Data?

4.5 Automated Decision and Profiling

## 4.1 Job candidates – What information we collect and how?

**How is data collected?**

Entering into the process of providing and making data available is voluntary; however, processing of your data is required in order to conduct the recruitment process. If you do not provide us with your personal data or you do not consent that your data is processed, you may not participate in the recruitment process.

**We collect your personal data when**:

- you submit it yourself, for example when you send your CV or other application documents by traditional or electronic means directly to us,
- you use different systems and applications that allow you to apply for a job;
- received from third parties, such as recruitment agencies, head-hunters or other employees or associates of BackB Investments S.à r.l. who provided your data upon your request and/or with your consent.

**What types of data are processed?**

- name and surname;
- image;
- telephone number, e-mail address, skype contact and personal address;
- date of birth, nationality and sex;

- date of interview and proposed job position;
- information about the expected remuneration;
- work permit in case of foreigners;
- the degree of adaptation to the current employment position and to the culture of the organisation;
- stimulus to the employment decisions and information on motivation to change job;
- education (name of school/year of graduation), degree, vocational title, scientific title, supplementary education, courses, post-graduate studies, specialisation, expertise and occupation;
- the progress of employment so far;
- knowledge of foreign languages, additional qualifications, driving licence, skills and hobbies;
- availability and notice period at the current workplace;
- any other information provided on CV.

## 4.2 Job candidates – Why we use your information and how we do it legally?

**We collect and use your data for the following purposes**:

- recruitment and evaluation of job applicants / candidates;
- internal reporting on the recruitment process;
- maintaining a database of potential candidates and ensuring a person's participation in further recruitment processes.

For recruitment purposes, we process your personal data because you have given us consent, in accordance with Article 6(1)a GDPR.

In this case, you may always withdraw your consent to the entire processing to which you have consented, or to specific purposes at your discretion, at any time. Withdrawal of consent will not affect the lawfulness of processing based on your consent prior to its withdrawal.

**What are your rights:**

- You have the right to request access to your personal data.
- You also have the right to request that your personal data is corrected, that your personal data is deleted and that the processing of your personal data is restricted.
- You have the right to object to the processing if the collection and use of the data is based on our legitimate interest. In the event of your objection, we will stop further processing of your personal data, unless we prove that there are valid legal grounds for further processing.
- You are also entitled to lodge a complaint with the national data protection supervisory authority (in Luxembourg, the CNPD - Commission Nationale pour la Protection des Données).

If your personal data is processed for other purposes, you will be informed thereof.

**Do we transfer your personal data outside the European Economic Area (EEA):**
Your data may be transferred to entities belonging to B2 Impact Group in third countries only after an adequate level of protection has been ensured and in accordance with the applicable laws.

An adequate level of protection will be ensured through technical measures and the signature of standard contractual clauses or on the basis of a decision of the European Commission establishing an adequate level of protection in the country concerned.

### 4.3 Job candidates – Who are the recipients of your data?

We may disclose your personal data for legitimate purposes to:

- entities belonging to B2 Impact Group, other than BackB Investments S.à r.l., in case where making such data available is necessary for the hiring decision;
- other entities in the event that a new entity is created, or the organisation is acquired by another entity if the controller is involved in the merger, sale or transfer of part or all of its business;
- other entities in the event that the entity is required to do so, for example pursuant to a court order or a legal provision in force;
- any other entities in the case of receiving consent from the job applicant / candidate (e.g. to verify previous employment positions).

### 4.4 Job candidates – How long do we keep your data?

We retain data for different periods of time for each recruitment process and purpose.

The retention period for data processed for recruitment purposes shall be the period remaining until the end of the year in which the recruitment is completed.

In the case of data collection for the processing of personal data for future recruitment processes, the data retention period is 3 years until the end of the year in which the last contact with the candidate took place.

### 4.5 Job candidates – Automated decision and profiling

BackB Investments S.à r.l. does not carry out profiling and does not apply automated decision-making for the purposes presented in this information notice.

# 5. Who we share your data with?

At times, it's necessary for us to share your personal data with others to fulfil our legal and contractual obligations and to pursue our legitimate interests, we may share the data with our affiliates, subsidiaries, or service providers to facilitate our business activity.

The following are examples of possible categories of recipients of your data:

| | |
|---|---|
| **Service Providers** | These are companies that assist us in managing our business activity, including technical support, email hosting, cloud solutions, security and risks management tools, data analysis, and IT services. These partners are contractually bound to comply with our data privacy and security requirements, ensuring the protection of your personal information. They are authorized to access personal data solely for the purposes we specify, contributing to the efficiency and security of our services. |
| **Professional Advisors** | We might work with lawyers, accountants, auditors, or consultants who could access your data while providing their services. |
| **Legal and Regulatory Authorities** | Occasionally, legal obligations may require us to share email data with law enforcement, regulators, or government authorities. |
| **Business Transfers** | If we undergo a merger, asset sale, or significant organizational change, your email data may be transferred to the new entity or owners. |
| **Third-Party Tools and Platforms** | We use various third-party tools and platforms to enhance our processes. These tools may process your email data on our behalf. |

| | |
|---|---|
| **Other Authorized Recipients** | There might be other authorized recipients we have to share data with, depending on specific situations and laws, |

We take measures to ensure the security and confidentiality of your data when shared.

# 6. International data transfers

We may need to transfer your data to countries outside the European Economic Area (EEA) or places with different data protection rules. We take steps to protect your data, including:

- **Adequacy Decisions**: If the European Commission says a country has good data protection, we can send data there without extra safeguards, including EU-US Data Privacy
- **EU-US Data Privacy Framework:** The European Commission has approved data transfers from the European Economic Area (EEA) to the United States under the EU-US Data Privacy Framework. Under this framework, your personal data may be transferred to participating U.S. companies without the need for additional safeguards.
- **Standard Contractual Clauses**: We might use these approved contracts to ensure your data is safe when it goes outside the EEA.

The information about the transfers can be obtained through the “Contact Us” section in the Privacy Policy.

# 7. How do we protect your data?

While performing our business activity, we are dedicated to ensuring the security of your personal data. We employ a range of technical and organizational measures to maintain the integrity and confidentiality of your personal information, protecting it from unauthorized access, disclosure, loss, alteration, or destruction.

| | |
|---|---|
| **Organizational Safeguards** | We have put in place various organizational measures, including policies, procedures, and guidelines that govern data protection practices across our organization. We regularly assess data processing activities to identify and mitigate risks to your privacy, ensuring a balanced approach. |
| **Data Encryption** | We use encryption techniques to safeguard your personal data during transmission and storage, rendering it impervious to unauthorized access or interception. |
| **Access Controls** | Strict access controls are firmly in place to guarantee that only authorized personnel have access to your personal data. Access privileges are granted on a need-to-know basis and are routinely reviewed and updated. |
| **Data Minimization** | We only collect and process personal data that is necessary for the purposes outlined in this Privacy Policy. The data collected is limited to what is necessary and relevant. |
| **Privacy from the Start** | We integrate data protection into our processes from the very beginning, using privacy-enhancing technologies and practices to uphold the highest standards of data protection and privacy. |
| **Employee Training** | We make sure our team knows how to keep your data safe through training. |
| **Incident Response** | In the unlikely event of a data breach or security incident, we have procedures in place to promptly respond, investigate, and mitigate the impact. We will notify you and the relevant authorities as required by applicable regulations. |

| | |
|---|---|
| **Regular Assessments** | We conduct regular assessments and audits of our data protection and security measures to identify and address any vulnerabilities or risks related to personal data. This helps us maintain the effectiveness of our security controls and ensure ongoing data protection. |
| **Other** | Other security measures required to manage the confidentiality, availability, and integrity of the data, aligned with the technology development. |

While we implement these technical and organizational measures, we are committed to continuously improving our security practices and adapt to evolving threats to safeguard your personal data. If you have any concerns about the security of your personal data or if you suspect any unauthorized access or disclosure, please contact us immediately using the contact details provided in the "**Contact Us**" section.

# 8. Your rights

We are committed to transparency and ensuring that your data subject rights are accessible and cost-free:

| | |
|---|---|
| **Right to Withdraw Your Consent at any time** | You can withdraw your consent for the processing of your Personal Data at any time. |
| **Right to Be Informed** | You have the right to be informed about how your Personal Data is collected and processed. This includes knowing the purposes of processing, who is processing your data, and how long it will be kept. |
| **Right to Object to Processing** | When we process your Data based on public or legitimate interest, you can object to it. |
| **Right to Access Your Data** | You can find out if we process your Data, get details about the processing, and a copy of your Data. |
| **Right to Rectify Your Data** | You have the right to ensure that your Personal Data is accurate and to request corrections if necessary. |
| **Right to Restrict the Processing of Your Data** | You have the right, under certain circumstances, to restrict the processing of your Data. In this case, we will not process the Data for any purpose other than storing it. |
| **Right to have Your Data Erased or otherwise removed** | You have the right, under certain circumstances, to obtain the erasure of your Data. |
| **Right to Portability of Your Data** | You can receive your Data in a structured, machine-readable format and, if possible, have it sent to another controller. This right applies when your Data is processed automatically, based on your consent, a contract, or pre-contractual obligations. |
| **Right Not to Be Subject to Profiling and Automated Decision-Making** | You have the right not to be subjected to solely automated decision-making processes, including profiling, that significantly affect you. This means that important decisions, such as those related to your rights, benefits, or legal matters, should not be made solely by automated systems without human intervention. This right safeguards against unfair or discriminatory automated decisions. |
| **Right to Lodge a complaint** | You have the right to bring a claim before the National Commission for Data Protection (Commission nationale pour la protection des données) at https://cnpd.public.lu/en/particuliers/faire-valoir/formulaire-plainte.html or directly to the court. |

**Limitations or Exceptions to Data Subject Rights:**
While we respect your rights, legal or legitimate reasons may prevent us from fulfilling some requests. For

instance, if it conflicts with our legal obligations or others' rights. We'll explain why if we can't fulfil your request.

**Withdrawing Your Consent**
You can withdraw your consent at any time. To do so:

- **Opt-Out:** For non-essential cookies, adjust your settings in your device or browser. Essential cookies for security will still be active.
- **Unsubscribe:** If you receive our newsletters or marketing communications, unsubscribe via the provided link.

Consent withdrawal may affect your experience:

- If you withdraw consent for non-essential cookies, some website features and personalized content may not be available to you. This may affect your overall user experience on our website.
- If you unsubscribe from our newsletter, you will no longer receive our news or updates about our services.

Withdrawing consent does not affect the lawfulness of any processing that occurred before your withdrawal. We are committed to respecting your choices and privacy preferences.

To request any action regarding your rights, contact us by email at dpo@b2upi.com or by postal mail to our head office. Our Data Protection Officer (DPO) will assist you and respond as soon as possible, not later than three months.

# 9. Privacy policy updates

We may update this Privacy Policy from time to time to reflect changes in our privacy practices or legal obligations. We will post the revised version on our website and update the "Effective Date" at the top of this policy. We encourage you to check our Privacy Policy periodically for the latest information on our privacy practices.

We are committed to keeping you informed about our data practices and any updates to our privacy policy. You can access the history of previous versions of this privacy policy by visiting the **"Privacy Policy History"** section on our website. This section provides a record of all previous versions, allowing you to review any changes made over time.

# 10. Key legal and technical terms used in the privacy policy

Here are several definitions for the key terms and legal notions used in our Privacy Policy to ensure clarity. These definitions aim to help you better understand the terminology used in this Privacy Policy.

If you have any further questions or need clarification on any terms or provisions, please don't hesitate to contact us. Your understanding of your data rights and our practices is essential to us.

| | |
|---|---|
| **Personal Data** | Any information about you, such as your name, email, or other identifying information that can directly or indirectly identify you as an individual. |
| **Data Processing** | The actions performed on personal data, including but not limited to collection, storage, organization, alteration, use, disclosure, or erasure. |

| | |
|---|---|
| **Data Processed** | The specific personal data we collect, use, or otherwise process according to this Privacy Policy. |
| **Data Controller** | That's us; we are responsible for determining how and why data is processed, and we ensure compliance with data protection laws. |
| **Data Subject** | An individual whose personal data is being processed. This term often refers to you, our Website User or Business Partner. |
| **Consent** | Your voluntary and informed agreement for us to process your data for specific purposes, obtained through clear and transparent means. |
| **Legitimate Interests** | One of the legal bases for processing personal data indicating that we have valid reasons for data processing that don't compromise your rights or interests. |
| **Profiling** | Automated data processing for the purpose of analysing and predicting behaviour, preferences, or interests, often used to personalize user experiences, perform risk assessments, or for analytics. |
| **Automated Decision-Making** | Decisions made solely by machines or automated systems, without human intervention, which may impact individuals' rights and freedoms. |
| **Data Protection Officer (DPO)** | An appointed individual responsible for overseeing data protection compliance within our organization and acting as a point of contact for data-related inquiries. |
| **Security Measures** | Proactive actions and safeguards taken to protect your data from unauthorized access, disclosure, alteration, loss, or destruction. |
| **International Data Transfers** | The process of sharing data across borders outside the Economic European Area ("EEA"), which may require specific safeguards to ensure data protection. |
| **Adequacy Decisions** | Official approvals indicating that certain countries outside the EEA provide an adequate level of data protection, allowing for data transfers without additional safeguards. |
| **Standard Contractual Clauses** | Legally binding agreements established to ensure data protection when personal data is transferred outside the EEA to entities that may not have equivalent data protection laws. |
| **Opt-In/Opt-Out** | The act of choosing to agree (opt-in) or disagree (opt-out) with specific data processing activities, such as subscribing or unsubscribing to our newsletters, or for cookies and tracking technologies. |
| **Cookies** | Small pieces of data stored on your device to enhance your web browsing experience, including tracking preferences and user behaviour for various purposes. |
| **Geographic Position** | Information about the approximate location of a user, such as their country and city, often collected with user consent for location-based services. |
| **Due Diligence** | The process of conducting research and assessments to evaluate the suitability and credibility of potential business partners, ensuring they align with our business objectives and standards. |
| **Data Subject Rights** | Your legal rights regarding your personal data, including the right to access, rectify, erase, restrict processing, object to processing, and data portability. |
| **Data Encryption** | The process of converting data into code or cipher to protect its confidentiality and integrity during transmission and storage. |
| **Access Controls** | Mechanisms and policies in place to manage and control who has access to specific data, limiting access to authorized individuals. |
| **Data Minimization** | The practice of collecting only the data that is necessary for the specified purposes of processing, minimizing the amount of personal data collected. |
| **Privacy by Design and Default** | Making privacy a priority during its processing. An approach that incorporates data protection and privacy considerations into the design and operation of systems and processes by default. |
| **Retention of Your Data** | Storing or using your data for specific periods during which we store or use your data for specific purposes, in compliance with legal and regulatory requirements. |
| **Purposes** | Specific and transparent reasons for processing personal data, outlined in this Privacy Policy or provided to you when obtaining your consent. |

| | |
|---|---|
| **Legal Basis** | The lawful justification for processing personal data, ensuring that processing aligns with applicable data protection laws. |
| **Legal Obligation** | Processing personal data due to applicable laws, regulations, or legal obligations. |

| Version | Date | Description |
|---|---|---|
| 1.0 | 06.05.2024 | Creating the document |