Recruitment Privacy Policy B2 Impact ASA

Effective Date: 29.09.2023

B2 Impact ASA ("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) and Law on the Processing of Personal Data (Personal Data Act) of 15 June 2018.

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 and use during the recruitment process.

Data Controller	**B2 Impact ASA** is a Leading Pan-European Debt Specialist providing debt solutions for banks and institutional vendors. Our vendors and business partners can rely on our solid industry experience, and trust that we aim for best practice in all our activities.
Contact Details	**Visiting Address:** Cort Adelers gate 30, 7th floor, 0245 Oslo, Norway **Phone:** +47 22 83 39 50 **Email:** post@b2-impact.com, dpo@b2-impact.com **Website:** www.b2-impact.com
Contact Us	If you have any questions, concerns, comments, or requests regarding this Privacy Policy or our data practices, please contact us to dpo@b2-impact.com.

Table of Contents

1. Who does this Privacy Policy apply to

This **Recruitment Privacy Policy** applies to all individuals who interact with us during the recruitment and hiring process. This includes, but is not limited to, job applicants, candidates, and prospective employees seeking employment opportunities with **B2 Impact ASA**.

B2 Impact ASA (the "Company" and the "Data Controller") processes your data with the purpose of the recruitment, processing, and assessment of your application for a position in the Company or our Group Companies.

For some processing activities, **B2 Impact ASA** and any of the affiliates of the Company (the "Group Companies") may process your personal data in a joint controlling relationship, when for the level of the position, your application should be assessed by any of the Group of Companies. You can find the Group Companies' data **here**.

By submitting your personal information and engaging with our recruitment process, you consent to the practices outlined in this policy.

Please take the time to carefully review this policy to understand how we collect, use, and safeguard your personal data. If you have any questions or concerns about this policy or our data handling practices, please don't hesitate to contact us using the information provided in this document.

2. What information is collected 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 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 recruitment process and professional interactions, such as your name, contact details, professional information, and other relevant documents or information.
- **Indirect collection from accepted third parties.** We may collect information about you from third parties like your former employers, when you provide your consent for checking your professional references.
- **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 recruitment process.

What categories of data are processed?

During our recruitment process, we may process personal data necessary for the recruitment and employment process. The specific personal data collected may vary depending on the nature of the position you apply for and the applicable particular requirements for the envisaged

position. We are committed to handling all data with care and in accordance with applicable data protection laws and regulations by ensuring adequate safeguards.

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

Identification Information	This category encompasses personal information such as your name, surname, date of birth, home address, residence, nationality, citizenship, identity card or passport data (e.g., CNP, series, and ID/passport number), or other identification data included in your CV and/or any recruitment-related forms.
Contact Details	This includes your correspondence address, telephone number, and email address.
Signature and Photo	Information included in the documents provided during the recruitment process, such as your signature and photo.
Demographic Data	We may collect data about your age, gender, and, if required for certain positions, the existence or type of driving license.
Data on Professional Experience	Information related to your occupation/profession, nature of the activities involved, previous employment, including periods of employment, work positions, names and addresses of previous employers, details related to your significant projects and achievements in your professional history.
Education Data and Professional Certifications	Details about your educational background, such as the name and type of graduated studies, educational institutions attended (schools and universities), duration, specialization, diplomas, studies, certifications, and participation in training programs and conferences.
Data on Professional Skills and Competences	Information about foreign languages known or used and computer skills as mentioned in your CV.
Data on Remuneration, Legal Fees, and Taxes	Specifics regarding the salary or remuneration requested, bonuses, benefits, and data on taxes and duties applicable according to tax legislation.
Communication Records	Records of email correspondences, meeting minutes, call logs, and other communication-related data exchanged during our professional interactions, like text, attachments, documents, images, and any other information shared during our correspondence, including communication with recruitment companies or former employers, as part of the recruitment process.
Data Resulting from Video Recording (Image and Voice)	Only in limited cases where video recordings are made during online interviews, only based on your consent.
Candidate Evaluation Data	This category comprises opinions and resolutions of authorized personnel involved in the recruitment process, references, interview notes, records/results of pre-employment verifications, and more.
Former Employers References	Details regarding professional activities and duration of employment obtained from former employers, based on your consent.
Data on Potential Conflicts of Interest	Information about the existence of kinship or affinity relations with employees or persons in the management of our Company, Group Companies our Business Partners, etc.
Regulatory Data	Data related to regulatory requirements, certifications, licenses, permits, accreditations, and industry-specific qualifications obtained by you and required for the position you applied for.
Dispute/Complaints Records Data Subjects Requests Records	Information related to any complaints, data subjects' requests and legal disputes that may arise during our recruitment process.
Audit and Compliance Data	Data related to audits, assessments, or inspections conducted by / or related to the recruitment process to ensure compliance and quality.
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 our 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.
Other Relevant Data	Any additional personal data voluntarily provided by you during interviews and correspondence to address specific requests or queries.
Sensitive Data	By exception, in the context of our recruitment process, sensitive data is only processed in specific situations where necessary to fulfil the recruitment process or required for specific executive positions. Sensitive data we may process includes: ▪ **Health Data Related to Occupational Medicine**: Information about certain special medical conditions or details of possible disabilities, including labor restrictions and/or special requirements. For selected candidates, health data related to occupational medicine and assessment of working capacity. ▪ **Data Regarding Disciplinary Sanctions**: Data regarding disciplinary sanctions for which the prescription period has not expired. ▪ **Data Regarding Restrictions/Prohibitions on the Exercise of Certain Professions**: Applicable for certain positions. ▪ **Data Regarding Political and Public Exposure**: If applicable.

Obligation to Provide Personal Data during Recruitment Process

We request personal data from our candidates to fulfil key purposes such as recruitment, competence evaluation, compliance checks, and employment. The consequence of not providing this required data may include limited recruitment opportunities and an impact on our further employment relationship:

Non-provision of necessary data may restrict access to specific positions or employment.

The absence of critical data may constrain our ability to finalize the recruitment process and initiate an employment relationship.

We value data accuracy and reliability, ensuring transparency and ethical standards in our collaborations. We encourage our candidates to provide the required personal data to facilitate effective recruitment assessment and mutually beneficial employment relationships.

3. 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
Identifying Eligible Candidates	Identifying candidates suitable for the position.	Taking steps to enter employment contract. Legitimate Interest to fill in existing vacancies.
Conducting Job Interviews	Arranging and conducting job interviews.	Taking steps to enter employment contract.
Competence Evaluation	Analysing candidates' profiles, both professional and personal.	Taking steps to enter employment contract Legitimate interest to suitable selection.

Verification Legal Conditions	Ensuring candidates meet legal requirements for specific positions (certifications, licenses, permits, accreditations, and industry-specific qualifications).	Legal Obligation
Facilitating Communication	Facilitate communication through various channels and correspondence between you and our Company.	Taking steps to enter employment contract Legitimate Interest to communicate with you for recruitment-related matters.
Obtaining References	Collecting references from former employers.	Consent (Could be withdrawn at any time)
Responding Your Inquiries	To respond to your inquiries, questions, or requests.	Taking steps to enter employment contract
Employment Documentation	Creating necessary employment-related documents.	Taking steps to enter employment contract
Maintaining Records and Documentation	To respond to legal requests. Keeping records and documents related to recruitment (in physical and/or electronic formats).	Legal obligation Legitimate Interest - demonstrate compliance and fairness of the process.
Conflict of Interest Assessment	To assess potential conflicts of Interest between our Company and candidates to ensure transparency and ethical conduct.	Legitimate Interest in maintaining transparency and ethical conduct in professional collaborations
Maintaining Candidate Databases	Building and maintaining a database of potential candidates for future recruitment.	Consent (Could be withdrawn at any time)
Prior Occupational Medicine Procedures	Assessing the health and working capacity of selected candidates.	Legal obligation
Interview Panels / Multi-Interviewer Assessments	To facilitate the evaluation process when multiple interviewers are participating, ensuring fairness and consistency in their assessments.	Consent (Could be withdrawn at any time) Legitimate Interest in conducting a fair and effective interview process
Establish Remuneration	To determine salary expectations, benefits, and tax-related information.	Taking steps to enter employment contract
Dispute Resolution	To facilitate resolution, investigations, or legal proceedings, in the event of any disputes arising.	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. 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 Legitimate interests in ensuring security and prevent fraud and illicit activities.
Research and Development	We may use aggregated data for research and development purposes to enhance our recruitment activity.	Legitimate interests in improving activity
Internal Analyses and Recruitment Strategy	We may process data to analysing and optimizing the recruitment process, developing recruitment strategies.	Legitimate interests in maintaining and improving our recruitment process and strategy.

Protecting the Company's Reputation and Interests	Safeguarding the reputation and interests of the Company, including prudent risk management	Legitimate Interest in protecting reputation
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	Only processed when necessary for specific situations or for executive positions as required.	Legal obligation if case Legitimate Interest to demonstrate compliance, establish, defend, and execute our rights in court.

Please note that the specific purposes and legal grounds for processing your personal data may vary depending on the context and your engagement with our recruitment process. We consistently adhere to relevant data protection regulations and uphold your privacy rights with the utmost care.

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.

4. How long do we keep your data?

We retain your data as long as needed for the execution of our recruitment process. We 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.

In the context of our recruitment process, personal data is typically retained for 6 months after the recruitment process is completed, primarily for audit purposes. However, data may be retained beyond this initial period under the following circumstances:

- Based on candidate consent, data may be retained for a duration of up to 3 years for further recruitment opportunities.
- In cases of security breaches, data breaches, or integrity incidents (whistleblowing), data may be retained for up to 3 years.
- Data may be retained for longer periods in response to requests from authorities as required by law.
- In situations of court litigation or ongoing disputes, data may be retained for 3 years following the resolution of the dispute or litigation.

- Following the exercise of the right to restrict processing, data may be retained until the restriction period concludes.

We ensure that any extension of data retention is carried out in compliance with applicable data protection regulations and with due consideration for privacy and security safeguards.

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.

5. 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. Our decision-making processes are based on human intervention and assessment to ensure fairness and individual consideration.

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 environment.
- **Analysis of Soft Skills and Personal Competences:** We may apply soft profiling techniques to assess soft skills and personal competencies of candidates during the recruitment process. It's important to note that this profiling involves human intervention and evaluation, ensuring that assessments are made with care and consideration. Soft profiling of candidates allows us to gain insights into their soft skills and personal competencies, which are valuable for determining their suitability for specific roles. This assessment complements the traditional evaluation process by providing a more comprehensive understanding of a candidate's qualifications and potential fit within our Company. Importantly, human intervention in this profiling process ensures fairness and individualized consideration, enhancing the quality of our recruitment decisions.

In all profiling contexts, the logic is to provide improved security, compliance, efficiency, and efficient interactions. The envisaged consequences are generally positive and aim to enhance the overall experience and outcomes for our professional relationships. 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.

6. Third-party services and tools

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 candidates. The types of data shared may vary depending on the

specific tool or service in use but can include information necessary for our recruitment process and professional cooperation.

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.

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

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

Our Group Companies	When for the level of the position, your application should be assessed by any of the Group of Companies. You can find the Group Companies' data here.
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,

8. 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.

9. 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.

10. 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 the 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 Norwegian Supervisory Authority at https://www.datatilsynet.no/en/ 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

If you have provided consent for specific purposes outlined in this Privacy Policy, you have the right to withdraw your consent at any time. To do so, please contact us immediately using the contact details provided in the "Contact Us" section or the dedicated consent management tools, if available. Please note that 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.

- **Obtaining References:** If you choose to withdraw your consent for obtaining references, please be aware that this may limit our ability to obtain relevant information about your professional background, potentially affecting our assessment of your suitability for a particular role. However, it will not affect your participation in our recruitment process or your eligibility for other positions.
- **Interview Panels / Multi-Interviewer Assessments:** You have the right to withdraw your consent for interview recording. However, please note that withdrawing consent may limit the efficiency of the recruitment process. We may need to conduct multiple discussions and meetings, potentially extending the time required to finalize the assessment and evaluation of candidates. This may also limit our ability to provide a comprehensive evaluation in a single meeting, leading to further discussions among interviewers.
- **Maintaining Candidate Databases:** If you decide to withdraw your consent for maintaining your data in our candidate database, we will promptly remove your information from our records. This means that we will no longer consider you for future recruitment opportunities, and you may need to reapply if you wish to be considered for new positions.

To request any action regarding your rights, contact us by email at dpo@b2-impact.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.

11. 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.

12. Key legal/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.