General Website Privacy Policy – B2 Impact A/S

Effective Date: 17/02/2026

B2 Impact A/S ("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, underline 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	**B2 Impact A/S** is part of B2 Impact Group, a Leading Pan-European Debt Specialist providing debt solutions for banks and institutional vendors, with portfolios in various European countries. **B2 Impact A/S** focuses on the management of debt portfolios in the Danish market.
Contact Details	**Visiting Address:** Bryggernes Plads 14, 4, 1799 København **Post Address:** Bryggernes Plads 14, 4, 1799 København **Email:** info@b2-impact.dk **Website:** www.b2-impact.dk **Phone:** 70 20 27 55
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.dk.

Table of Contents

1. Website Users Privacy Policy

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 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 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 do 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
Ensuring 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 Contact Form 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 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	The 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. 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, analyse user behaviour, 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 analyse 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. 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 fulfil 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.

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 behaviour, 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 behaviour, 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 s t a n d a r d s 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.

<end of chapter>

2. Email Exchange Privacy Policy

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

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

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 you choose to share 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 Legitimate interest
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

Responding to Inquiries	We may process your personal data to respond to inquiries, questions, or requests made via email.	Contract execution Legitimate interest
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 it at any time).*).
Customizing User Experiences	We may process data related to your email interactions to personalize and improve your user experience.	Legitimate interest
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 interest
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 obligation Legitimate interest
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 interest
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 obligation Legitimate interest
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.	Legal obligation Legitimate interest
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 Legitimate interest
Risk Management and Control Activities	To assess, manage, and control risks related to data security, privacy, and compliance.	Legitimate interest
Sensitive Data Processing	To process sensitive data voluntarily provided by you during email exchanges for specific purposes as agreed upon.	Consent Legitimate interest

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.

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.

<end of chapter>

3. Privacy Policy - Customers involved in Debt Collection

This Privacy Policy applies to all our customers, who have a debt owned and/or managed by us and are connected to the debt collection process.

These categories may include debtors, co-payers, guarantors, mortgage guarantors, adjudicators, potential and final buyers of the collaterals owned or managed by us. We also process personal data related to legal and/or conventional proxies and representatives of these categories.

For our debt collection cases we entered into a joint-controlling agreement with the affiliated entity in our Group:

Joint controller 1	B2 Impact ASA
Headquarter	Cort Adelers gate 30, 0254 Oslo, Norway
Phone number	+47 22 83 39 50
Email address	dpo@b2-impact.com
Joint Controller 2	Ultimo Portfolio Invest (Luxembourg) S.A.
Headquarter	9, rue Joseph Junck, L-1839 Luxembourg
Phone number	N/A
Email address	dpo@b2upi.com
Website	https://www.b2-impact.com/

The rights and responsibilities presented in this Privacy Policy could be executed towards both the above-mentioned Joint Controllers.

3.1. Customers: What information we collect and how?

How is data collected?

We collect your personal data using various methods to make our professional interactions, collaborations, and security more efficient. If you decide to share information about other individuals during the debt collection process, please be aware that you are responsible for any third-party Personal Data obtained and shared with us. You also confirm that you have obtained the third party's consent to provide such data to us.

Methods of Collection:

- **Direct Collection** includes information you provide like data directly shared by you during the debt collection process and professional interactions, such as your name, contact details, debt-related information, and other pertinent documents or information.
- **Indirect Collection**. We may collect your data from interested third parties or from publicly available sources like public official databases or registers if such information is relevant to our contractual relationship and debt collection process.

The possible sources that we may indirectly collect data from include:

- Your initial or current creditor, such as financial institutions or mobile network operators, with whom you have signed the credit or service agreements. They may assign their claim rights to us or authorize us to manage debt collection on their behalf.
- In certain cases, from individuals who have a legitimate interest related to the contract for which we are conducting debt collection activities.
- From individuals authorized by you to communicate with us on your behalf or those making payments on your behalf.
- From public authorities and institutions, or other entities providing services of public interest, such as bailiffs, courts, or public notaries.
- From publicly available publications and databases, or those based on contractual relationships (external sources). This is done to ensure continuous updates and verification of the data we have about you, or to assess your ability to repay the debt. External sources may include public institutions and authorities, registers, public electronic databases, information available on social media, the internet, or from third parties. These third parties may include, but are not limited to, Public Official Population Register, the National Trade Register, Tax Authority, and third parties authorized to hold databases of individuals subject to international sanctions or politically exposed individuals.
- From our contractual partners to whom you have provided your data to conclude a contract with us or to purchase collateral for claims managed by us (like real estate companies or websites).

If you have any questions or need further clarification about how we collect and handle your data, please feel free to Contact Us. Your understanding of our data collection methods is important to us.

What types of data are processed?

During our debt collection process, professional interactions, and collaborations, we gather various types of personal data essential for managing debts properly.
The specific data collected depends on the nature of our contractual relationship, interactions, and the purposes behind them. We take your privacy seriously and handle all data with care and in accordance with relevant data protection laws and regulations.

Below, we present the main categories of personal data we may process:

Categories of Data	Details On Personal Data Processed
Identification Information	Name, contact details (like phone, email and mailing addresses), personal identifiers (e.g., Social Security number or national ID), ID cards details and any other identification information shared during debt collection process and relevant for our cooperation.
Debt Related Data	Information about the debts, value, number, loan or service agreement, past and current transactions, such as payment history, amount owed, due dates, interest accrued, etc. Information about your payment history with other creditors, if available. Information about any other debts or financial obligations you may have with us or other creditors.
Payment Arrangements and Debt Settlement	Information about any payment arrangements, repayment plans, debt settlement or agreements negotiated with you.
Communication Records Interaction History	Records of email correspondences, correspondence related to debt, letters, call logs, and other communication-related data exchanged during debt collection process. Data related to your past interactions with us, such as previous communication logs, call recordings, or notes from customer service representatives.
Voice and Call Recordings	Recordings of calls made to or received from you for quality assurance and dispute resolution purposes (voice).
Communication Preferences	Data about your preferences for language and communication channels, such as email, phone calls, or postal mail.
Legal Information	Legal status and information resulting from legally binding documents, such as loan agreements, service contracts, and any other documentation that provides evidence of the debt.
Credit Information	We may obtain data related to your credit history, credit reports, and credit scores from credit bureaus/registers or other sources.
Financial Information Asset and Liability Information	Payment information, financial transactions records, including bank account details, credit ratings, payment terms, financial transactions, payment history, invoices, data related to your financial statements, including income, expenses, and other financial data relevant to your debt management. Information about your assets, liabilities, and overall financial position.
Financial Hardships	Data related to any financial hardships or circumstances affecting your ability to repay the debt
Bankruptcy or Insolvency	Information about any bankruptcy or insolvency proceedings related to you, or your discharge from bankruptcy proceedings, if applicable.
Debt Collection Action Records	Details of any debt collection action taken, including court proceedings and engagement with collection agencies.
Collateral Data	Information related to any collateral provided by you to secure the debt, such as property details or other assets information.
Demographic Data	Information about your demographics, such as age, gender, marital status, and household composition.
Professional and Business Information Employment Status	This category includes information like current employment status, employer details, and income source, business registration information and tax ID number.
Dispute Records	Information related to any legal disputes, complaints or challenges related to the debt that may arise during debt collection process.
Debt Collection Analytical Data	Analytical data related to your payment behaviour to predict payment patterns and segment debts and portfolios based on characteristics. Data related to your behaviour, preferences, and debt collection patterns, which might influence debt collection strategies. Data related to your behaviour and interactions with our website or digital platforms.

Collection Performance Metrics	Data resulting from collection performance metrics to optimize collection efforts (including data from analysing channel effectiveness, conversion rates, and operational efficiency).
Screening Data Against Sanctions and PEP Lists	Data resulting from screening against official sanctions lists and databases of politically exposed persons. This includes identification data and may reveal sensitive information related to political exposure/opinions, criminal convictions or alleged offences, where such information is included in official or authoritative sources.
KYC and AML Data	Information related to Know Your Customer (KYC) and Anti-Money Laundering (AML) checks and assessments performed on you to detect and prevent money laundering activities (may include sensitive data related to criminal convictions, regulatory complaints and investigations involving you, or fraudulent activities).
Third-Party Data	Data obtained from third-party debt collection agencies or agents involved in the debt collection process. Data obtained from third-party sources, such as skip tracing services, for locating debtors.
Conflict of Interest Data	Data related to the assessment of potential conflicts of interest involving our Employees or Business Partners.
Risk Assessment Data	Information related to the risk assessment of our customers, considering factors such as financial stability, reputation, and compliance history.
Whistleblowing Reporting	Data related to whistleblowing processes and investigations, including reports, interviews, evidence, and findings.
Regulatory Data	Data related to regulatory requirements, certifications, licenses, permits and accreditations.
Insurance Data	Information about the insurance coverage (if applicable).
Marketing Preferences	Preferences for marketing communications, feedback, survey results, and other marketing-related data shared during our interactions.
Geographical Location	Information about your geographical location, which can help determine jurisdiction and relevant legal actions.
Feedback and Surveys	Feedback and satisfaction surveys provided by you during the debt collection process. Customer insights and satisfaction data to help tailor personalized offers and enhance your experience.
Audit and Compliance Data	Data related to external/interna. audits, assessments, or inspections related to the debt collection process to ensure compliance and quality.
Access Rights and Permissions	Data about the access rights and permissions granted to you on our platforms.
Technical and Device Data	Technical information and device data used to access our platforms, system and application access logs, IP addresses, and the usage of digital resources relevant to our interactions.
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 various elements, including timestamps, user identifiers, system activity records, access logs, IP addresses, WhatsApp ID (if applicable), 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	Customer type, Customer industry and depending on your interactions, we might process additional personal data, such as information related to our events information, or contractual terms and any other data relevant to our professional relationship.

Sensitive Data	Sensitive data, like health or special needs information, is used only when provided voluntarily to assess eligibility for certain payment options or discounts. During Sanction/PEP screening process, we may collect and process data related to criminal convictions, fraudulent activities, or politically exposed person (PEP) status. The processing of sensitive data follows relevant data protection laws. The objective is to meet legal requirements and uphold ethical standards while respecting individuals' rights and freedoms.

Obligation to Provide Personal Data for Our Business Relationship

We request personal data from our customers - including debtors, co-payers, guarantors, mortgage guarantors, adjudicators, potential and final buyers of the collaterals owned or managed by us, as well as legal and/or conventional proxies and representatives of these categories.

This data is essential for various purposes, including the debt collection process, risk assessment, compliance checks, and collaborations. While we may collect certain data from other sources, not providing the required data directly may have consequences.

Consequences of Not Providing Required Data:

- **Restricted Access**: Non-provision of necessary data may limit your access to specific services, resources, or information related to the debt collection process.
- **Impact on Debt Payment Resolution**: The absence of critical data may impact on our ability to effectively manage and resolve your debt in line with your needs, potentially leading to delays or challenges in the debt collection process.
- **Limited Debt Settlement Options**: In cases where debt settlements or negotiations are necessary for debt resolution, the absence of essential data may constrain our ability to engage in mutually beneficial payment agreement that could facilitate debt settlement.

We are committed to ensuring data accuracy and reliability in our debt collection process, adhering to transparency and ethical standards. We encourage all Customers to provide the required personal data directly to us to facilitate the efficient management of their debts and, where applicable, to help achieve mutually agreeable solutions. Please be aware that data obtained from other sources may be outdated and/or inaccurate, potentially affecting the effectiveness of the debt collection process. Your cooperation in providing accurate and up-to-date information is highly appreciated and contributes to a smoother debt resolution process.

3.2. Customers - 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, along with the legal bases for each purpose.

Purpose	Details on the Purpose	Legal Base
Managing Debt Collection Process	Efficient debt collection and business operations.	Legal Obligation Contract Execution Legitimate Interest
Debt Payments Payments Reconciliation and History	Process financial transactions, billing, payments, and related financial activities necessary for the debt collection process.	Contract Execution Legal Obligation
Communication	Facilitate communication with you for debt collection-related matters through various channels and correspondence between you and our company.	Contract Execution Legitimate Interest

Voice Recording	Performing Call Centre activities or ensuring redline whistleblowing reporting.	Consent (for Voice) Contract execution Legitimate Interest Legal Obligation
Responding to Your Inquiries	Responding to your inquiries, questions, or requests.	Contract execution Legitimate Interest Legal Obligation
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 it at any time).*
Record Keeping and Compliance	Ensuring record-keeping, regulatory requirements, and responding to legal requests.	Legal Obligation Legitimate Interest
Sanctions/PEP Screening	Screening against International Sanctions public official lists and PEP databases, to ensure compliance with applicable international and national sanctions regimes and prevent prohibited business relationships or transactions.	Legal Obligation Legitimate Interest *(Please check the details in the next section)*
Know Your Customer (KYC) and Anti-Money Laundering (AML)	Conducting due diligence and assessments to prevent money laundering, terrorist financing and fraudulent activities.	Legal Obligation Legitimate Interest
Customers Risk Assessment	Assessing financial and other relevant risks related to Customers' financial stability, reputation, and compliance history.	Legal Obligation Legitimate Interest
Prevention Conflict of Interest	Analysing potential conflicts of interest to ensure transparency and ethical conduct.	Legitimate Interest
Whistleblowing Process	Ensuring proper analysis and investigation of all whistleblowing reports submitted by internal or external stakeholders.	Legal obligation Legitimate Interest
Checking Regulatory Requirements	Verifying necessary certifications, licenses, permits, and industry-specific qualifications (if necessary).	Legal Obligation
Marketing and Surveys	To manage marketing preferences, feedback, survey results, and other marketing-related data shared during our interactions.	Consent *(You have the right to withdraw it at any time).*
Dispute Resolution	In the event of disputes arising from our debt collection process, we may process relevant personal data to facilitate resolution, investigations, or legal proceedings for the establishment, exercise, or defence of legal claims.	Legitimate Interest
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. To document complaints and data subjects' requests management and to ensure the establishment, exercise, or defence of legal claims.	Legal Obligation Legitimate Interest
Eligibility for special payment settlements or discounts	By exception, in the context of our relationship and only based on your requests, we may process certain sensitive data regarding your health condition or special needs, in specific situations in order to establish and document eligibility criteria for special payment settlements or discounts.	Consent Legal Obligation

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. Protecting our business from fraud and maintaining the security of our business operation.	Legal Obligation Legitimate Interest
Research and Development	Aggregated data for research and development purposes to enhance our services and activity and to improve our debt collection process.	Legitimate Interest
Business Analytics and Reporting	Reviewing data for business analytics, reporting, and performance assessment, for monitoring our debt collection process and business operations.	Legitimate Interest
Service Performance Evaluation Monitoring Business Development	To monitor and evaluate the quality of our services, identify areas for improvement, and enhance business or to identify potential business opportunities, collaborations, or partnerships.	Legitimate Interest
Internal Audit External Audit Compliance Monitoring	To conduct internal and external audits and ongoing compliance monitoring to ensure that our company adheres to regulatory requirements, policies, and internal standards.	Legal Obligation Legitimate Interest
Risk Management and Control Activities	To assess, manage, and control risks related to data security, privacy, and compliance aiming to ensure proper risk management, sustainability, and compliance of our operations.	Legitimate Interest

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. Customers - Specific Information on Sanctions/PEP Screening

The following section supplements the general Customers (Debtors) Privacy Policy and applies only to the sanctions and politically exposed persons (PEP) screening process. It explains how and why your personal data is processed for mandatory screening purposes, including the applicable legal grounds, data sources, screening logic, and possible consequences.

3.3.1. Purposes and Legal Grounds of Sanction/PEP Screening

We perform Sanctions / PEP Screening to comply with applicable international, European Union, and national laws on international sanctions and restrictive measures, anti-money laundering (AML) and counter-terrorist financing (CTF).

The primary objectives of this screening are:

- ensuring compliance with applicable international and national sanctions regimes.
- preventing money laundering, terrorist financing, and sanctions circumvention.
- performing legally required due diligence and ongoing monitoring

- preventing prohibited business relationships or transactions
- ensuring lawful and responsible conduct of our debt collection activities.
- protecting the integrity, security, and lawful operation of our business.

Our processing is based on legal obligations (GDPR Article 6(1)(c)), our legitimate interests (Article 6(1)(f)), and specific conditions for processing data related to sanctions listings and criminal offences under Article 10 GDPR and applicable national AML/sanctions laws. Limited categories of special data regarding political exposure are processed only in connection with official listings under Article 9 of GDPR.
Sanctions & PEP Screening is a mandatory compliance activity and is not used for marketing or unrelated profiling purposes.

3.3.2. Personal Data Categories, Data Subjects and Sources of Data

During the screening process, we collect and process only data strictly necessary to execute the screening process such as:

- **Customers**: The personal data we process for the screening may include full name, contact details, date of birth, gender, nationality, citizenship, country of residence, internal customer ID, and, where necessary to assess a potential match, limited business or financial information directly linked to the screening outcome. We collect this data directly from you during our business relationship or indirectly from the initial vendors or from public registers and sources.
- **Individuals included in Sanctions lists**: The personal data we process for the screening may include full name and listed aliases, date and place of birth, gender, nationality, citizenship, country of residence, official identifiers, contact details, listed public function or profession, sanctions or PEP-related information published by competent authorities, like source and sanctioning authority, sanctioning details; specific goods or services that are subject to sanctions; information on the grounds for listing (statement of reasons), possibly including criminal records or proceedings; other relevant public available information, necessary for effective sanction screening.

Data Sources include public official information consolidated and provided by specialized third-party screening sources based on:

- Official sanction lists, issued by public authorities (EU, UN, national authorities, other relevant international organizations).
- PEP datasets derived from public and authoritative sources
- Publicly accessible regulatory, governmental, and international databases
- Other credible sources, including regulatory bodies, law enforcement, and international organizations.

We do not control the content of official sanctions or PEP lists or the information in public records or data sets used by third-party screening providers. Responsibility for the accuracy, scope, and publication of such data lies with the issuing public authorities. Public bodies determine what personal data is disclosed, balancing public interest with individual privacy rights.

3.3.3. Screening Criteria and Possible Consequences in case of a Positive Match

Screening activity involves comparing identification data of our customers against official sanctions and PEP lists using predefined matching criteria. We utilize advanced and secure technology and algorithms to ensure accurate and efficient screening as well as data confidentiality, integrity, and availability.

- If a potential match is identified, it is reviewed manually by authorized personnel, additional checks may be performed to confirm or clear the match, no adverse decision is taken automatically by any system, without proper and diligent human review.
- If a confirmed match is determined after additional case review, the business relationship may be restricted, suspended, or terminated, transactions or contractual steps may be blocked or delayed, reporting or escalation to competent authorities may be required by law. We ensure strict compliance with all applicable legal requirements in managing these outcomes.

3.3.1. Data Retention

We keep personal data from sanctions and PEP screening only for as long as required by law and only to the extent strictly necessary.

- Sanctions and PEP lists are used only during checks for potential matching and are automatically deleted after screening execution.
- Only information related to a possible or confirmed match (for example, that a check was performed, the result, and the review decision) is kept for compliance and audit purposes.
- Screening results, supporting evidence, and audit records are usually kept for the minimum period required under AML/CFT laws (typically 5 years). This period may be extended only if required for an ongoing investigation, regulatory request, or legal claim.
- Once the applicable retention period expires, the data is deleted or anonymised.

3.3.4. Data Sharing

Personal data may be accessed or shared with competent public authorities, where required by law, with our Group entities providing centralized technical screening services and service providers supporting screening operations, acting under strict contractual data-protection obligations. We do not share personal data with any third party for marketing purposes.

3.3.5. Data Subjects Rights regarding Sanction/PEP Screening

In connection with the screening processing activity, you have the rights provided by the GDPR regarding your personal data, including the right to access, rectify and erase your information. You may also have the right to object to or restrict the processing of your personal data in certain circumstances.
Please note that certain rights may be restricted where necessary to comply with sanctions, AML/CFT laws or regulatory confidentiality obligations. Any restriction of your rights is assessed case by case and documented.
You can exercise your rights or contact the Data Protection Officer using the contact details provided in this Privacy Policy.

3.4. Customers -Third-Party Services and Tools

While managing our debt collection process, we may utilize various third-party tools and services to enhance our operations and facilitate effective debt collection services. These tools and services are designed to streamline processes, improve debt management, communication, and support the secure processing and exchange of information.

Our suite of third-party tools and services may encompass a diverse array of functionalities and solutions, including Customer Relationship Management Systems (CRMs), cloud solutions, email platforms, and other similar tools. These technologies enable us to collaborate efficiently while upholding data security standards.

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

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.

3.5. Customers - How long do we keep your data?

We retain your data as long as needed for the execution and management of the debt collection process and generally up to **5 years** after the debt is fully repaid/closed or after all enforcement legal proceedings are completed.
In certain cases, the data may be retained for longer period, **up to 10 years** if other legal deadlines apply.

Additionally, the personal data could be processed and retained as long as required to secure our legitimate interest in case of any litigation.
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. Customers - 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. Rest assured that your rights and interests are safeguarded through our manual review and human intervention in decision-making processes.

Profiling: We employ profiling techniques in various contexts to optimize our operations, enhance efficiency, and tailor our services to better meet your needs. Below are the key profiling activities we perform, along with their respective rationales and safeguards:

- **Debt Portfolio Performance Analysis** techniques involve analysis of data related to the performance of the debt portfolio, including trends and historical data. The objective is to optimize debt collection strategies and identify performance trends. It helps in making data-driven decisions to improve debt collection services. Consequences include enhanced debt collection strategies, improved services, and more effective debt resolution processes.
- **Efficiency Analysis of Debt Collection Process** involves techniques meant to streamlining the debt collection process by analysing relevant data. It aims to reduce errors and enhance the overall efficiency of debt collection. It assists in making the debt collection process smoother and error-free. Consequences include a more efficient and streamlined debt collection process, resulting in reduced delays and errors.
- **Identification of Payment Behaviour Patterns** involves analysing data to identify patterns in debtors' payment behaviour. It is used to tailor debt collection strategies based on observed payment patterns. The insights gained help in customizing debt collection approaches. The outcome of such profiling includes more effective and tailored debt collection services, aligned to our Customers' needs.
- **Analysis for the initiation of Legal Enforcement Proceedings** is based on profiling techniques which provide relevant information to support the decision-making process concerning initiation of legal enforcement proceedings and the most of suitable approach depending on specific debt details. The goal is to ensure compliance with legal requirements when initiating legal actions and to identify most suitable solutions for the managed debts. Profiling assists in making informed decisions about the necessity and appropriateness of legal enforcement proceedings, including bailiff enforcement. Human intervention is integral to this decision-making process, providing oversight and accountability, guaranteeing that all legal proceedings are carried out with precision and in adherence to regulatory guidelines.
- **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.
- **Risk Assessment and Due Diligence Profiling** techniques are employed to assess and manage risks related to Customers, 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 the debt collection process. 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. Profiling results are reviewed by human intervention to ensure alignment with ethical standards and regulatory requirements.

- **Performance Profiling** techniques help us to assess our performance and service quality by analysing performance metrics, service level agreements, and feedback data. It aids in evaluating and enhancing the efficiency and effectiveness of our debt collection activities. Consequences include better service quality and more efficient interactions tailored to meet both our needs. Human experts oversee and validate the outcomes of profiling to maintain transparency and fairness.
- **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.

None of the profiling activities described above result in decisions that produce legal effects or similarly significant consequences for you. In all profiling contexts, the overarching objective is to create a safer, more transparent, and highly efficient environment for debt collection activities.

These profiling techniques play an essential role in achieving several key goals. They enhance security by identifying potential risks and vulnerabilities, ensure compliance with regulatory requirements, streamline processes for increased debt collection efficiency, and enable personalized interactions tailored to Customers' preferences.

The envisaged consequences are consistently positive, resulting in improved data security, strengthened compliance, optimized operational efficiency, and a more personalized and satisfactory experience for our Customers, ultimately contributing to successful debt management outcomes for both parties.

Please be assured that all 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.

<end of chapter>

4. Business Partners Privacy Policy

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

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

4.1. 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 to us 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/PEP Screening Data	Data resulting from screening against official sanctions lists and databases of politically exposed persons. This includes identification data and may reveal sensitive information related to political exposure/opinions, criminal convictions or alleged offences, where such information is included in official or authoritative sources.
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	During Sanction/PEP screening process, we may collect and process data related to criminal convictions, fraudulent activities, or politically exposed person (PEP) status. The processing of sensitive data follows relevant data protection laws. The objective is to meet legal requirements and uphold ethical standards while respecting individuals' rights and freedoms.

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.

4.2. 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 cooperation process, along with the legal bases 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 Legitimate interest
Billing and Payments	Process financial transactions, billing, payments, and related financial activities necessary for our collaborations.	Contract execution Legal obligation
Facilitating Communication	Facilitate communication through various channels and correspondence between you and our organization.	Contract execution Legitimate interest
Responding to Your Inquiries	We may process your personal data to respond to your inquiries, questions, or requests.	Contract execution
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
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 Legitimate interest *(Please check the details in the next*

		section)
Know Your Customer (KYC) 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 Legitimate interest
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
Checking Regulatory Requirements	To verify necessary certifications, licenses, permits, and industry-specific qualifications obtained by our Business Partners.	Legal obligation Legitimate interest
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 Legitimate interest
Service Performance Evaluation	To evaluate the performance and service quality of our Business Partners, including service level agreements and feedback.	Legitimate interest
Marketing and Surveys	To manage marketing preferences, feedback, survey results, and other marketing-related data shared during our interactions.	Consent
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 interest
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 obligation Legitimate interest
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 obligation Legitimate interest
Research and Development	We may use aggregated data for research and development purposes to enhance our services and activity.	Legitimate interest
Business Analytics and Reporting	We may analyse data for business analytics, reporting, and performance assessment.	Legitimate interest
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 interest
Internal /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 Legitimate interest
Risk Management and Control Activities	To assess, manage, and control risks related to data security, privacy, and compliance.	Legitimate interest

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.

4.3. Business Partners: Specific Information on Due Diligence Process

The following section supplements the general Business Partners Privacy Policy and applies only to the sanctions and politically exposed persons (PEP) screening process. It explains how and why your personal data is processed for mandatory screening purposes, including the applicable legal grounds, data sources, screening logic, and possible consequences.

4.3.1. Purposes and Legal Grounds of the Screening

We perform Sanctions / PEP Screening to comply with applicable international, European Union, and national laws on international sanctions and restrictive measures, anti-money laundering (AML) and counter-terrorist financing (CTF).

The primary objectives of this screening are:

- ensuring compliance with applicable international and national sanctions regimes.
- preventing money laundering, terrorist financing, and sanctions circumvention.
- performing legally required due diligence and ongoing monitoring
- preventing prohibited business relationships or transactions
- ensuring lawful and responsible conduct of our debt collection activities.
- protecting the integrity, security, and lawful operation of our business.

Our processing is based on legal obligations (GDPR Article 6(1)(c)), our legitimate interests (Article 6(1)(f)), and specific conditions for processing data related to sanctions listings and criminal offences under Article 10 GDPR and applicable national AML/sanctions laws. Limited categories of special data regarding political exposure are processed only in connection with official listings under Article 9 of GDPR.
Sanctions & PEP Screening is a mandatory compliance activity and is not used for marketing or unrelated profiling purposes.

4.3.2. Personal Data Categories, Data Subjects and Sources of Data

During the screening process, we collect and process only data strictly necessary to execute the screening process such as:

- **Our Business Partners**: The personal data we process for the screening may include full name, contact details, date of birth, gender, nationality, citizenship, country of residence, and, where necessary to assess a potential match, limited business or financial information directly linked to the screening outcome. We collect this data directly from you during our business relationship or indirectly from public registers and sources.

- **Individuals included in Sanctions lists**: The personal data we process for the screening may include full name and listed aliases, date and place of birth, gender, nationality, citizenship, country of residence, official identifiers, contact details, listed public function or profession, sanctions or PEP-related information published by competent authorities, like source and sanctioning authority, sanctioning details; specific goods or services that are subject to sanctions; information on the grounds for listing (statement of reasons), possibly including criminal records or proceedings; other relevant public available information, necessary for effective sanction screening.

Data Sources include public official information consolidated and provided by specialized third-party screening sources based on:

- Official sanction lists, issued by public authorities (EU, UN, national authorities, other relevant international organizations).
- PEP datasets derived from public and authoritative sources
- Publicly accessible regulatory, governmental, and international databases
- Other credible sources, including regulatory bodies, law enforcement, and international organizations.

We do not control the content of official sanctions or PEP lists or the information in public records or data sets used by third-party screening providers. Responsibility for the accuracy, scope, and publication of such data lies with the issuing public authorities. Public bodies determine what personal data is disclosed, balancing public interest with individual privacy rights.

4.3.3. Screening Criteria and Possible Consequences in case of a Positive Match

Screening activity involves comparing identification data of our business partners against official sanctions and PEP lists using predefined matching criteria. We utilize advanced and secure technology and algorithms to ensure accurate and efficient screening as well as data confidentiality, integrity, and availability.

- If a potential match is identified, it is reviewed manually by authorized personnel, additional checks may be performed to confirm or clear the match, no adverse decision is taken automatically by any system, without proper and diligent human review.
- If a confirmed match is determined after additional case review, the business relationship may be restricted, suspended, or terminated, transactions or contractual steps may be blocked or delayed, reporting or escalation to competent authorities may be required by law. We ensure strict compliance with all applicable legal requirements in managing these outcomes.

3.3.6. Data Retention

We keep personal data from sanctions and PEP screening only for as long as required by law and only to the extent strictly necessary.

- Sanctions and PEP lists are used only during checks for potential matching and are automatically deleted after screening execution.
- Only information related to a possible or confirmed match (for example, that a check was performed, the result, and the review decision) is kept for compliance and audit purposes.
- Screening results, supporting evidence, and audit records are usually kept for the minimum period required under AML/CFT laws (typically 5 years). This period may be extended only if required for an ongoing investigation, regulatory request, or legal claim.
- Once the applicable retention period expires, the data is deleted or anonymised.

4.3.4. Data Sharing

Personal data may be accessed or shared with competent public authorities, where required by law, with our Group entities providing centralized technical screening services and service providers supporting screening operations, acting under strict contractual data-protection obligations. We do not share personal data with any third party for marketing purposes.

4.3.5. Data Subjects Rights regarding Sanction/PEP Screening

In connection with the screening processing activity, you have the rights provided by the GDPR regarding your personal data, including the right to access, rectify and erase your information. You may also have the right to object to or restrict the processing of your personal data in certain circumstances. Please note that certain rights may be restricted where necessary to comply with sanctions, AML/CFT laws or regulatory confidentiality obligations. Any restriction of your rights is assessed case by case and documented. You can exercise your rights or contact the Data Protection Officer using the contact details provided in this Privacy Policy.

4.4. 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.

4.5. 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.

4.6. 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.

<end of chapter>

5. Who Do 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 Group entities and 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.

<end of chapter>

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.

<end of chapter>

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.

<end of chapter>

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	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 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 Object to Processing	When we process your Data based on public or legitimate interest, you can object to it.
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 or to protect our rights in court.
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 Data Portability	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 Danish Supervisory Authority at https://www.datatilsynet.dk/ 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 link provided.

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@b2-impact.dk 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.

<end of chapter>

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.

<end of chapter>

10. Key Legal and Technical Terms in this 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, our Client 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 of European Commission 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.

<end of document>