PRIVACY AND DATA PROCESSING POLICY

B2KAPITAL PORTFOLIO MANAGEMENT SRL

Date of entry into force: [date **of publication on the website must be included]**

B2KAPITAL PORTFOLIO MANAGEMENT SRL ("we", "us" or "our") is committed to protecting the privacy and security of your personal data, as well as the rights and freedoms of data subjects, in accordance with the European General Data Protection Regulation (GDPR). The basic principles of personal data processing: legality, transparency, purpose limitation, data minimization, accuracy, storage limitation, confidentiality, integrity and responsibility, are the basis of our business activities. This Privacy Policy explains how we collect, use, disclose and protect the personal data we collect through our website, while providing our services and during our daily business.

Data Controller	**B2KAPITAL PORTFOLIO MANAGEMENT SRL** is a debt collection company that offers debt collection services consisting of all amicable and judicial recovery operations and procedures
Contact details	**Headquarters:** Metropolis Center, 89-97 Grigore Alexandrescu Street, Building A, 7th floor, Sector 1 **Phone:** +40 372 391 790 **Email:** privacy@b2kapital.ro; b2romania@B2kapital.ro **Website:** https://b2kapital.ro/
Contact Us	If you have any questions, concerns, comments, or requests regarding this Privacy Policy or our data practices, please contact us to privacy@b2kapital.ro

PRIVACY POLICY – MAIN CHAPTERS

1. PRIVACY POLICY OF SITE USERS

This privacy policy applies to users of our website.

Website Content Website User 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 personal data of third parties obtained, published or shared through this website and confirm that they have the consent of the third party to provide us with the data.

Data collection

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

The data collection methods we use may include:

- **Voluntarily Received Information –** Data you share with us when you interact with our site and choose to share some personal information by filling out forms, subscribing to our newsletters, or interacting with our content.
- **Automatic information**: We may automatically collect data 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.

The categories of personal data processed when you visit our website may include the following types of data, collected by us 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 website	We do not track what you do on our website, such as the pages you visit, what links you click on, and other actions.
Cookies	We use cookies and similar technologies to personalize your experience, to remember your preferences
Contact Information	If you choose to contact us through our website, 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 answer your questions, provide support, and keep you up to date with the latest news.

Registration data	When you visit our website, we may ask for your permission to use non-essential cookies, which are small text files placed on your device. These cookies help us to improve our website and provide a personalised experience. You have the ability to accept or decline these cookies. Your preferences are stored so that we know whether or not to use them when you visit our website. You can adjust your cookie settings at any time via your device or browser settings. Please note that some cookies, such as those necessary for website security, will remain active.
Demographic information	If you choose to provide them, we may collect information about your age, gender, location, or preferences.
Geographical position	We may collect your location. (such as your country and city) with your permission. This helps us provide location-based services and improve your website 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 required data	Depending on your interactions, we may process additional personal data, such as identifying information, user-generated content, usage data, contact details, incident reports, and more.

When you visit our website, we do not collect financial information, social security numbers, or sensitive personal data through our website. We only collect what is necessary for the purposes we have explained in our Privacy Policy. We process your personal data. with your consent, for our legitimate interests in improving our website and services and to comply with legal obligations.

Obligation to provide personal data

Users of the site are not obliged to provide personal data. Data collection is mainly based on voluntary sharing and consent. In addition, some data, such as technical information related to essential cookies, may be collected automatically during visits to the website 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 provide a personalized experience. Users may receive more generic content and may not benefit from tailored recommendations.

1.2. WEBSITE USERS – WHY WE USE YOUR PERSONAL INFORMATION AND HOW DO WE DO IT LEGALLY?

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

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

Purpose	Details of the purpose	Legal basis	Data processed
Website Security	We process your personal data. to protect the security of our website, prevent unauthorised access and stop fraudulent activities.	Legitimate interest	IP addresses, device information, browser information, website usage

			data, clickstream data, and session information.
Online payments	We ask for your personal data, such as your name and email address. This data is transmitted to the payment processor (EuroPayment Services S.R.L.)	Consent	Contact information: (name, email)
Cookie consent registration	We ask for and record your consent for non-essential cookies and manage cookie preferences to comply with legal requirements.	Legal obligation Legitimate interest	Recording Your Consent for non-essential cookies, cookie preferences, device and browser information, IP address.
Data retention	We process data to comply with legal obligations, such as record-keeping requirements, data retention and deletion requirements	Legal obligation	Deletion of data collected after the expiration of the retention period.
Reply to Legal requests	We process data to respond to legal requests, such as court orders or law enforcement investigations.	Legal obligation	All personal data collected through our website
Cookies and Tracking Technologies	We collect data about your activities, preferences, and interactions. navigation through cookies and similar technologies.	Consent (Unless strictly necessary)	Cookies, IP address, device information, browser information, website usage data.
Monitoring and auditing	Monitoring and auditing purposes, such as internal or external audits, conformity assessments, compliance with security standards.	Legitimate interest	Identification information, documentation, audit logs, records, compliance data.

1.3. THIRD-PARTY SERVICES AND TOOLS

We use third-party tools to improve the user experience: (Polylang for translation) and for security purposes (reCAPTCHA as an anti-spam solution).

For detailed information about these cookies and data management, please check the **Cookie Policy [insert link].** 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 personal data. for as long as necessary for legal reasons or for as long as necessary to fulfill the purposes outlined in this Privacy Policy.
The time we keep can change depending on things like:

- Type of data – Some data requires longer retention than others.
- The purposes for which we process your personal data.
- Legal and regulatory requirements. Sometimes the law says we need to keep the data.
- Our business needs and operational requirements affect how long we retain data.

We may be required to retain certain personal data for a longer period in order to comply with legal and regulatory obligations, resolve disputes, and exercise our rights.
During the retention period, we will take appropriate technical and organisational measures to ensure the security and confidentiality of your personal data. After 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
Cookies	Usually until you finish browsing or up to 12 months
Contact Information	For 3 years so that we can respond to and document your requests.
Other required data	Up to 3 years, depending on what data it is and what we have collected.

Please note that you have rights regarding your data, such as requesting to delete it in certain situations. To find out more about your rights and how to use them, please see the "Your Rights" section of the Privacy Policy.

1.5. AUTOMATED DECISION-MAKING AND PROFILING

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

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

- **Cookies** are used to collect data about user behavior, preferences, and interactions with our website. This data is valuable for understanding user preferences, providing personalized experiences, and improving website functionality.
- **Monitoring and audit-based security profiling** involves tracking user activities, access logs, and compliance data to ensure compliance with security standards and regulations. This is done to maintain the security and integrity of the website, to protect against unauthorized access, and to demonstrate compliance with legal requirements.

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

1.6. WHO DO WE SHARE YOUR DATA WITH?

Sometimes, it is necessary for us to share your personal data. To fulfill our legal and contractual obligations and pursue our legitimate interests, we may share data with our affiliates, subsidiaries, or service providers to facilitate our business activity.

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

Service providers	These are companies that help us manage our business, including technical support, email hosting, cloud solutions, security and risk management tools, data analytics, and IT services. These partners are contractually bound to comply with our data privacy and security requirements, ensuring the protection of your personal information. Personal. They are authorized to access personal data only for the purposes we specify, contributing to the efficiency and security of our services.
Professional advisors	We may work with lawyers, accountants, auditors or consultants who may have access to your personal 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 are going through a merger, asset sale or significant organizational change, your data will be can be transferred to the new entity or owners.
Tools and platforms offered by third parties	We use various third-party tools and platforms to improve our processes. These tools may process your email data on our behalf.
Other authorized recipients	There may be other authorized recipients with whom we need to share the data, depending on specific situations and laws,

We take steps to ensure the security and privacy of your personal data. when shared.

1.7. International data transfers

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

- **Adequacy decisions** : If the European Commission declares that a country has good data protection, we may send data there without additional 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. Within this framework, your personal data will be may be transferred to participating U.S. companies without the need for additional collateral.
- **Standard Contractual Clauses**: We may use these approved contracts to ensure that your data is secure when outside the EEA.

Information about transfers can be obtained through the "Contact Us" section of the Privacy Policy.

1.8. How do we protect your data?

In the course of our business, we are dedicated to ensuring the security of your personal data. Personal. We use a range of technical and organizational measures to maintain the integrity and confidentiality of your information. protecting them against unauthorized access, disclosure, loss, alteration, or destruction.

Organisational safeguards	We have implemented various organizational measures, including policies, procedures, and guidelines that govern data protection practices within 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 protect your personal data during transmission and storage, making it impervious to unauthorized access or interception.
Access controls	Strict access controls are firmly in place to ensure that only authorized personnel have access to your personal data. Personal. Access privileges are granted on a need-to-know basis and are reviewed and updated regularly.
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	From the beginning, we integrate data protection into our processes, using privacy-enhancing technologies and practices to maintain 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, in accordance with the applicable regulations.
Periodic evaluations	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.
Others	Other security measures necessary to manage the privacy, availability and integrity of data, aligned with the development of technology.

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

1.9. Your rights

We are committed to ensuring transparency and ensuring that your rights are met. data subject are accessible and free of:

The right to withdraw your consent at any time	You can withdraw your consent to 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 being used. are collected and processed. This includes knowing the purposes of the processing, who is processing your data, and who is processing your data. and how long they will be kept.
Right to object to processing	When we process your personal data. on the basis of public or legitimate interest, you can object.
Right of access to your data	You can find out whether we are processing your data, obtain details of the processing and a copy of your data.
Right to rectify your data	You have the right to ensure that your data is not subject to any are correct and ask for corrections if necessary.
The right to restrict the processing of your personal data	You have the right, under certain circumstances, to restrict the processing of your personal data. In this case, we will not process the data for any purpose other than storing it.
The right to delete your data or otherwise remove it	You have the right, in certain circumstances, to obtain the deletion of your personal data.
The right to portability of your data	You can receive your personal data. in a structured, machine-readable format and, if possible, you can send them to another operator. This right applies when your personal data is not applicable. are processed automatically, based on your consent, a contract or pre-contractual obligations.
The right not to be subject to profiling and automated decision-making	You have the right not to be subject exclusively to automated decision-making processes, including profiling, which significantly affect you. This means that important decisions, such as those related to your rights, benefits, or issues. should not be taken exclusively by automated systems without human intervention. This right provides protection against unfair or discriminatory automated decisions.
Right to lodge a complaint	You have the right to file an action before the Romanian Supervisory Authority at the address: Bd. G-ral Gheorghe Magheru 28-30, sector 1, postal code 010336, Bucharest, Romania, phone:+40318059211; email:anspdcp@dataprotection.ro on the page web: http://www.dataprotection.ro/ or directly to the court.

Limitations or exceptions to the rights of data subjects:

While we respect your rights, legal or legitimate reasons may prevent us from fulfilling some requests. For example, if it conflicts with our legal obligations or the rights of others. We'll explain why if we can't fulfill your request.

Withdrawal of consent

You can withdraw your consent at any time. To do this:

- **Opt-out:** For non-essential cookies, adjust the settings on your device or browser. Cookies that are essential for security will still be active.

Withdrawing consent may affect your experience:

- If you withdraw your consent to 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.

The withdrawal of consent does not affect the lawfulness of any processing that took place prior to your withdrawal. We are committed to respecting your privacy choices and preferences.

To request any action regarding your rights, please contact us by email at: dpo@veraltis.ro or by post at our head office. Our Data Protection Officer (DPO) will assist you and respond to you as soon as possible, no later than three months.

2. EMAIL EXCHANGE PRIVACY POLICY

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

- Customers (debtors)
- Customers and potential customers
- Investors
- Business partners, suppliers and external advisors
- Employees
- Candidates
- Legal authorities
- Other stakeholders involved in the email exchange process.

Content of the Email Exchange Privacy Policy

2.1. EMAIL EXCHANGE – WHAT INFORMATION DO WE COLLECT AND HOW?

How is the data collected?

We collect personal data through various means to facilitate our email exchange process and to ensure security.
If you choose to share information about others, please note that you are responsible for any personal data of third parties obtained and shared through the email exchange process and confirm the third party's consent to provide such data to us.

- **Direct collection** includes information you provide, such as data shared directly 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 such as 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 carried out. 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:

Identifying Information	Your name, contact details (such as phone and postal addresses), and any other personal information shared during email exchanges, such as 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 revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the unique identification of a natural person, health data or data on a natural person's sex life or sexual orientation, health-related information or other data classified as sensitive under applicable laws on data protection. Any sensitive data shared with us will be processed in accordance with the highest standards of data protection and only for the specific purposes for which it is provided by you.
Communication metadata logs and IT usage data	To investigate and document incidents, verify 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, records of financial transactions, payment details, bank account and invoices related to professional agreements, order history, and details of products or services discussed during email exchanges.
Other required data	Depending on your interactions, we may process additional personal data, such as information related to our professional agreements, project details, information about events or contractual terms, and any other data relevant to our professional relationship.

Please note that the specific categories of data processed during email exchanges may vary depending on the nature of the business interaction and the information you choose to share with us through the 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, the communication is usually initiated by you while providing your personal data. voluntarily by e-mail correspondence. Users are not obliged to provide such personal data for the exchange of emails. However, the absence of certain data may affect the effectiveness of email communication and limit our ability to respond to your questions. or to provide specific information.

2.2. EMAIL EXCHANGE - WHY WE USE YOUR PERSONAL INFORMATION AND HOW DO 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, together with the legal bases and categories of data processed for each purpose.

Purpose	Details of the purpose	Legal basis
Facilitating email communication	We process your personal data. to facilitate email communication and correspondence between you. and our organization.	Performance of the contract or taking steps to conclude a contract and/or Legitimate interest in communicating with you efficiently and effectively via email for business-related issues.
Compliance with legal obligations	We may process your personal data. to comply with legal obligations, including record keeping, regulatory requirements, and responding to legal requests.	Compliance with a legal obligation to which we are subject.
Answering questions	We may process your personal data. to respond to questions, queries or requests made by email.	Performance of the contract or taking steps to conclude a contract and/or Legitimate interest in communicating with you efficiently and effectively via email for business-related issues.
Personalization of user experiences	We may process data related to your interactions. by email to personalize and improve your experience. by the user.	Legitimate interests to provide you with a better and more personalized experience.
Research & Development, Business Analytics & Reporting	We may use aggregated email data for business analysis, reporting and performance evaluation, for research and development purposes to improve our services and business.	Legitimate interests in monitoring and improving our business operations
Fraud Prevention Incident Investigation Security Monitoring	We may process email, IT usage data, and logs to prevent fraudulent activities, unauthorized access, verify phishing emails, ensure security monitoring, and investigate and document security breaches, data breaches, or other incidents that may affect the security of your data. Personal.	Legal obligations to investigate and document incidents, and Legitimate interests in protecting our business from fraud and maintaining the security of email communications.

Litigation	In the event of disputes arising from email exchanges, we may process relevant personal data to facilitate legal settlement, investigations or proceedings.	Legitimate interests related to the establishment, exercise or defense of legal claims.
Complaint resolution Managing Data Subject Requests	To address and resolve complaints or concerns raised by you. or third parties about our services, processes or processing of our personal data and to respond to data subject requests.	Legal obligations to document and respond to complaints and requests from data subjects and/or Legitimate interests related to the establishment, exercise or defense of legal claims.
Improving services Business Development	We may process email data to monitor the quality of our services, identify areas for improvement, improve the overall user experience, identify potential business opportunities, collaborations, or partnerships.	Legitimate interests in maintaining and improving our services and pursuing the growth and development of the business.
Internal audit External audit compliance monitoring	To conduct internal and external audits and ongoing compliance monitoring to ensure that our organization adheres to regulatory requirements, policies, and internal standards.	Legal obligation and/or Legitimate interests
Risk management and control activities	To assess, manage, and control data security, privacy, and compliance risks.	Legitimate interests in ensuring the risk management, sustainability and compliance of our operations.
Processing of sensitive data	To process sensitive data voluntarily provided by you. during email exchanges for specific purposes as agreed.	Legitimate interests related to the establishment, exercise or defense of legal claims.

Please note that the specific purposes and legal bases for processing may vary depending on the circumstances and your interactions. with us. We always ensure that personal data is processed in accordance with applicable data protection laws and respecting your personal rights. Privacy Policy.
It is important to emphasise that when we process personal data for legitimate interests, we balance those interests with the rights and freedoms of the individuals whose data is being processed. We take steps to ensure that your rights are protected. are also respected that personal data is processed in a fair and lawful manner.

2.3. EMAIL EXCHANGE - THIRD-PARTY SERVICES AND TOOLS

We may use various third-party tools and services to optimize our email exchange process, ensuring effective 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 privacy requirements. Please note that our use of third-party tools is always aimed at improving the quality and security of our email exchanges.

2.4. EMAIL EXCHANGE – HOW LONG DO WE KEEP YOUR DATA?

We keep your personal data. for as long as it is necessary for communication by e-mail and mainly up to 3 years after the end of the e-mail exchange, for legal and dispute resolution purposes.
However, please note that in certain cases, depending on the subject and content of the email correspondence, the retention period may be longer depending on specific purposes and regulatory requirements.
For example, if we have a contractual relationship, we may retain the relevant data for up to 5 years after the contractual relationship has ended or if other legal terms apply.

We always ensure compliance with the relevant legal obligations and adjust our retention periods accordingly to meet these requirements. Our primary purpose is to retain data for as long as necessary to fulfill the purposes outlined in this privacy policy and to comply with any legal obligations.
During the retention period, we will take appropriate technical and organisational measures to ensure the security and confidentiality of your personal data. After the retention period expires, we will securely delete or anonymize your personal data. in accordance with applicable laws and regulations.

Please note that you have rights regarding your data, such as requesting to delete it in certain situations. To find out more about your rights and how to use them, please see the "Your Rights" section of the Privacy Policy.

2.5. EMAIL EXCHANGE - AUTOMATED DECISION AND PROFILING

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

Profiling activities in the email exchange process can only be used 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 protect 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 more efficient environment to engage in professional relationships. The importance lies in improving security. The expected consequences are generally positive and aim to improve the overall experience and results of our communication.

We assure you that any profiling activities are carried out in accordance with the relevant data protection laws and regulations. You have the right to object to profiling processes, if applicable.
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.

2.6. WHO DO WE SHARE YOUR DATA WITH?

Sometimes, it is necessary for us to share your personal data. To fulfill our legal and contractual obligations and pursue our legitimate interests, we may share data with our affiliates, subsidiaries, or service providers to facilitate our business activity.

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

Service providers	These are companies that help us manage our business, including technical support, email hosting, cloud solutions, security and risk management tools, data analytics, and IT services. These partners are contractually bound to comply with our data privacy and security requirements, ensuring the protection of your personal information. Personal. They are authorized to access personal data only for the purposes we specify, contributing to the efficiency and security of our services.
Professional advisors	We may work with lawyers, accountants, auditors or consultants who may have access to your personal 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 are going through a merger, asset sale or significant organizational change, your data will be can be transferred to the new entity or owners.
Tools and platforms offered by third parties	We use various third-party tools and platforms to improve our processes. These tools may process your email data on our behalf.
Other authorized recipients	There may be other authorized recipients with whom we need to share the data, depending on specific situations and laws,

We take steps to ensure the security and privacy of your personal data. when shared

2.7. International data transfers

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

- **Adequacy decisions** : If the European Commission declares that a country has good data protection, we may send data there without additional 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. Within this framework, your personal data will be may be transferred to participating U.S. companies without the need for additional collateral.
- **Standard Contractual Clauses**: We may use these approved contracts to ensure that your data is secure when outside the EEA.

Information about transfers can be obtained through the "Contact Us" section of the Privacy Policy.

2.8. How do we protect your data?

In the course of our business, we are dedicated to ensuring the security of your personal data. Personal. We use a range of technical and organizational measures to maintain the integrity and confidentiality of your information. protecting them against unauthorized access, disclosure, loss, alteration, or destruction.

Organisational safeguards	We have implemented various organizational measures, including policies, procedures, and guidelines that govern data protection practices within 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 protect your personal data during transmission and storage, making it impervious to unauthorized access or interception.
Access controls	Strict access controls are firmly in place to ensure that only authorized personnel have access to your personal data. Personal. Access privileges are granted on a need-to-know basis and are reviewed and updated regularly.
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	From the beginning, we integrate data protection into our processes, using privacy-enhancing technologies and practices to maintain 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, in accordance with the applicable regulations.
Periodic evaluations	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.
Others	Other security measures necessary to manage the privacy, availability and integrity of data, aligned with the development of technology.

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

2.9. Your rights

We are committed to ensuring transparency and ensuring that your rights are met. data subject are accessible and free of:

The right to withdraw your consent at any time	You can withdraw your consent to 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 being used. are collected and processed. This includes knowing the purposes of the processing, who is processing your data, and who is processing your data. and how long they will be kept.
Right to object to processing	When we process your personal data. on the basis of public or legitimate interest, you can object.
Right of access to your data	You can find out whether we are processing your data, obtain details of the processing and a copy of your data.
Right to rectify your data	You have the right to ensure that your data is not subject to any are correct and ask for corrections if necessary.
The right to restrict the processing of your personal data	You have the right, under certain circumstances, to restrict the processing of your personal data. In this case, we will not process the data for any purpose other than storing it.
The right to delete your data or otherwise remove it	You have the right, in certain circumstances, to obtain the deletion of your personal data.
The right to portability of your data	You can receive your personal data. in a structured, machine-readable format and, if possible, you can send them to another operator. This right applies when your personal data is not applicable. are processed automatically, based on your consent, a contract or pre-contractual obligations.
The right not to be subject to profiling and automated decision-making	You have the right not to be subject exclusively to automated decision-making processes, including profiling, which significantly affect you. This means that important decisions, such as those related to your rights, benefits, or issues. should not be taken exclusively by automated systems without human intervention. This right provides protection against unfair or discriminatory automated decisions.
Right to lodge a complaint	You have the right to bring an action before the Romanian Supervisory Authority at the address: 28-30 G-ral Gheorghe Magheru Blvd., sector 1, postal code 010336, Bucharest, Romania, telephone:+40318059211; e-mail:anspdcp@dataprotection.ro, on page b: http://www.dataprotection.ro/ or directly at the court.

Limitations or exceptions to the rights of data subjects:

While we respect your rights, legal or legitimate reasons may prevent us from fulfilling some requests. For example, if it conflicts with our legal obligations or the rights of others. We'll explain why if we can't fulfill your request.

Withdrawal of consent

You can withdraw your consent at any time. To do this:

- **Opt-out:** For non-essential cookies, adjust the settings on your device or browser. Cookies that are essential for security will still be active.

Withdrawing consent may affect your experience:

- If you withdraw your consent to 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.

The withdrawal of consent does not affect the lawfulness of any processing that took place prior to your withdrawal. We are committed to respecting your privacy choices and preferences.

To request any action regarding your rights, please contact us by email at dpo@veraltis.ro or by post at our head office. Our Data Protection Officer (DPO) will assist you and respond to you as soon as possible, no later than three months.

3. PRIVACY POLICY OF ASSOCIATED OPERATORS: Veraltis Asset Management SRL.-B2 Kapital Portfolio Management SRL.

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

Associated Operator 1: **Veraltis Asset Management S.R.L. ("VAM")** having its registered office in: 89-97 Grigore Alexandrescu Street, building A, 7th floor, sector 1, phone: +40 372 391 790 E-mail: contact@veraltis.ro; dpo@veraltis.ro Website: https://www.veraltis.ro

Signed an Associate Operators Agreement with another entity from the B2 Impact group:

Associated Operator 2: **B2 Kapital Portfolio Management SRL.(" B2KPM)** having its registered office in: 89-97 Grigore Alexandrescu Street, building A, 7th floor, sector 1, phone: +40 372 391 790 E-mail: contact@b2kapital.ro; privacy@b2kapital.ro Website: https://www.b2kapital.ro

VAM and **B2KPM** (together "we" or "controllers") currently manage your debit and will act as joint controllers in relation to the processing of your personal data.

Please find below the Information Notice on the processing of personal data, which aims to help you understand how we collect your personal data as a joint controller, what categories of information we process, why we process it, how we use it, how long we keep it, who we share it with and why, as well as your rights and how you can exercise them.

We process the personal data of our clients who have debts held by any entity of our Group and/or that are related to the debt collection process. These categories may include debtors, co-payers, guarantors, mortgage guarantors, adjudicators, potential and ultimate purchasers of collateral held or managed by us. We also process personal data relating to legal and/or conventional processors and representatives of these categories.

Content of the Customer Privacy Policy

3.1. CUSTOMERS - WHAT INFORMATION DO WE COLLECT AND HOW?

How is the data collected?

We collect your personal data through various methods to streamline our interactions, collaborations and professional security. If you decide to share information about others during the debt collection process, please note that you are responsible for any personal data of third parties obtained and shared with us. You also confirm that you have obtained the consent of the third party to provide us with such data. Exceptionally, we may also process information relating to individuals whose personal data is provided by individuals with whom a contractual relationship is established. In this case, we will take all reasonable steps to inform data subjects of the content of this notice regarding the processing of personal data.

Collection methods:

- **Direct collection** includes information that you provide, such as data shared directly 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, such as official public databases or registers, if this information is relevant to our contractual relationship and debt collection process.

Possible sources from which we may indirectly collect data include:

- Your lender Original or current, such as financial institutions or mobile network operators, with whom you have signed a credit or service agreement. They assigned their claim rights to BBSV, which authorizes us to manage the collection of claims on their behalf.
- In certain cases, from individuals who have a legitimate interest in the contract for which we carry out debt collection activities.
- From the persons authorized by you. communicate with us on your behalf. or those who make payments on your behalf.
- From public authorities and institutions or from other entities providing services of public interest, such as bailiffs, courts or notaries public.
- From publicly available publications and databases or those based on contractual relationships (external sources). This is done to ensure continuous updates and checks of the data we have about you. or to assess your ability to do so. to repay the debt. External sources may include public institutions and authorities, registers, public electronic databases, information available on social media, on the internet or from third parties. These third parties may include, but are not limited to, the Official Public Population Registry, the

National Trade Registry, the Tax Authority, and third parties authorized to hold databases of persons subject to international sanctions or politically exposed persons.

- From our contractual partners to whom you have provided your personal data. to enter into a contract with us or to purchase collateral for claims managed by us (such as real estate companies or websites).

If you have any questions or need further clarification about how we collect and handle your data, please do not hesitate 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 collect different types of personal data that are essential for the correct management of debts. The specific data collected depends on the nature of our contractual relationship, the interactions and the purposes behind them. We take your privacy seriously. and we handle all data with care and in accordance with relevant data protection laws and regulations.

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

Data categories	Details of the personal data processed
Identifying Information	Name, contact details (such as telephone, email address and postal addresses), personal identifiers (e.g. social security number or national ID), ID card details and any other identifying information shared during the debt collection process and relevant to our cooperation.
Debit data	Information about debts, value, number, loan or service agreement, past and current transactions, such as payment history, amount owed, due dates, accrued interest, etc. Information about payment history with other creditors, if available. Information about any other debts or financial obligations you have to us or other creditors.
Payment methods and Debt Extinguishment	Information about any payment methods, repayment plans, debt settlement, or agreements negotiated with you.
Recordings of communications Interaction history	Records of email correspondence, debt-related correspondence, letters, call logs, and other communication-related data exchanged during the debt collection process. Data about your interactions with us, such as previous communication logs, call recordings, or notes from customer service representatives.
Voice recordings and calls	Recordings of calls made or received from you for quality assurance and dispute resolution (voice).
Communication preferences	Data about your preferences for language and communication channels, such as email, phone calls, or 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 debt.

Financial information **Information on assets and liabilities**	Payment information, financial transaction records, including bank account details, credit ratings, payment terms, financial transactions, payment history, invoices, data related to your financial statements, etc. including income, expenditure and other financial data relevant to debt management. Information about your assets, liabilities and general financial position.
Financial difficulties	Data relating to any financial hardship or circumstances that affect your ability to repay debt
Bankruptcy or insolvency & foreclosure	Information about any bankruptcy or insolvency proceedings or foreclosures related to you or downloading your from the ASTFL of procedures, if applicable.
Records of debt collection actions	Details of any debt collection actions taken, including legal proceedings and working with collection agencies.
Collateral data	Information related to any warranty provided by you to secure debt, such as property details or other asset information.
Demographics	Information about demographic data, such as age, gender, marital status, and household composition.
Professional and business information **Professional status**	This category includes information such as current employment status, employer details and source of income, company registration information, and tax identification number.
Litigation	Information relating to any legal disputes, claims or debt-related challenges that may arise during the debt collection process.
Analytical data on debt collection	Analytics about your behavior to anticipate payment patterns and segment borrowers based on characteristics. Data about your behavior, preferences, and patterns debt collection strategy, which could influence debt collection strategies. Data about your behavior and interactions with our website or digital platforms.
Collection performance indicators	Data from collection performance indicators to optimize collection efforts (including data from channel effectiveness, conversion rates, and operational efficiency analysis).
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 activity).
Sanctions screening and PEP lists	Data from your verification in relation to official sanctions lists and databases of politically exposed persons (may include sensitive data related to political opinions, criminal convictions or fraudulent activities).
Data from third parties	Data obtained from third-party debt collection agents or agents involved in the debt collection process. Data obtained from third-party sources, such as skip tracing services, to locate debtors.
Conflict of interest data	Data relating to the assessment of potential conflicts of interest involving our employees or business partners.

Risk assessment data	Information related to our clients' risk assessment, taking into account factors such as financial stability, reputation, and compliance history.
Whistleblowing reporting	Data relating to whistleblowing processes and investigations in the public interest, including reports, interviews, evidence and findings.
Regulatory data	Data related to regulatory requirements, certifications, licenses, permits, and accreditations.
Insurance data	Information about insurance coverage (if applicable).
Geographical location	Information about your location geographical, which can help you determine the relevant jurisdiction and legal action.
Audit and compliance data	Data related to external/internal audit, 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 data about the devices used to access our platforms, system and application access logs, IP addresses, and the use of digital resources relevant to our interactions.
Metadata logs and IT usage data	We may collect metadata logs and information related to IT usage across different systems and applications. This data plays an important role in investigating and documenting incidents, verifying the authenticity of communications, and maintaining security measures. It can include various elements, including timestamps, user identifiers, system activity logs, access logs, IP addresses, WhatsApp IDs, device details, app usage logs, server logs, cloud data, and metadata associated with various interactions. In addition, this information helps monitor security and respond to incidents across our IT infrastructure, including but not limited to email systems, cloud environments, and other applications and software platforms integrated into our business operations.
Other relevant data	The type of customer, the industry of the customers and depending on your interactions, we may 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	By exception, in the context of our relationships, sensitive data is processed only in specific situations, which include: ▪ Information about your terms health or special needs – only if you have voluntarily provided to determine eligibility for special payments, settlements or discounts. ▪ Sanctions screening process where we may collect and process sensitive data related to criminal convictions, fraudulent activities or politically exposed person (PEP) status (if such information is disclosed in public official lists) as part of our sanctions screening procedures to ensure compliance with regulatory requirements and mitigate potential risks associated with individuals or entities.

	Please note that the processing of sensitive data is carried out with the utmost care and in strict accordance with applicable data protection laws. Our primary goal is to protect the rights and freedoms of individuals while fulfilling our legal obligations and maintaining the highest ethical standards in our professional relationships.

Obligation to provide personal data for our business relationship

We request personal data from our Clients – including debtors, co-payers, guarantors, mortgage guarantors, adjudicators, potential and final purchasers of collateral held or managed by us, as well as legal and/or conventional processors and representatives of these categories. This data is essential for various purposes, including the debt collection process, risk assessment, compliance checks and collaborations. Although we may collect certain data from other sources, failure to provide the requested data directly may have consequences:

Consequences of not providing the requested data:

- **Restricted access**: Failure to provide the necessary data may limit your access to certain services, resources, or information related to the debt collection process.
- **Impact on debt payment solutions**: The absence of critical data can affect our ability to effectively manage and resolve your debt according to your needs, which can lead to delays or challenges in the debt collection process.
- **Limited debt settlement options**: In cases where debt settlements or negotiations are necessary to resolve debts, the absence of essential data may limit our ability to engage in a mutually beneficial payment arrangement that could facilitate debt settlement.

We are committed to ensuring the accuracy and reliability of data in our debt collection process, while respecting transparency and ethical standards. We encourage all customers to provide us directly with the personal data requested in order to facilitate the effective management of their debts and, where appropriate, to help achieve mutually acceptable solutions. Please note that data obtained from other sources may be outdated and/or inaccurate, which may affect the effectiveness of the debt collection process. Your cooperation in providing accurate and up-to-date information is highly valued and contributes to an easier debt settlement process.

3.2. CUSTOMERS - WHY WE USE YOUR INFORMATION AND HOW DO WE DO IT LEGALLY?

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

Purpose	Details of the purpose	Legal basis
Debt management **Collection process**	Efficient debt collection and business operations.	Legal obligation Performance of the contract Legitimate interest
Payment of debts **Payment reconciliation and history**	Processing of financial transactions, invoicing, payments, and related financial activities required for the debt collection process.	Performance of the contract Legal obligation

Communication	Facilitating communication with you for issues related to debt collection through various channels and correspondence between you. and our company.	Performance of the contract Legitimate interest
Voice recording	Responding to your requests, questions or requests.	Consent (You have the right to withdraw it at any time).
Answering your questions	Responding to your requests, questions or requests.	Performance of the contract Legitimate interest
Record Keeping and Compliance	Ensuring that records, regulatory requirements and response to legal requests are maintained.	Legal obligation Legitimate interest
Verification of sanctions	Checking clients against official public lists of international sanctions. As part of our sanctions verification procedures, we may collect and process sensitive data related to criminal convictions, fraudulent activities, or politically exposed person (PEP) status (if such information is disclosed in official public lists) to ensure compliance with regulatory requirements and mitigate potential risks associated with individuals or entities.	Legal obligation Legitimate interest *(Please check the details below in the next section)*
Know Your Customer (KYC) and Anti-Money Laundering (AML)	Conducting due diligence and assessments to prevent money laundering and fraudulent activities.	Legal obligation Legitimate interest
Customer Risk Assessment	Assessment of financial and other relevant risks related to clients' financial stability, reputation and compliance history.	Legal obligation Legitimate interest
Prevention of conflicts of interest	Analysis of potential conflicts of interest to ensure transparency and ethical conduct.	Legitimate interest
Whistleblower process	Ensuring proper analysis and investigation of all whistleblowing reports submitted by internal or external stakeholders.	Legal obligation Legitimate interest
Verification of regulatory requirements	Verification of required industry-specific certifications, licenses, permits, and qualifications (if required).	Legal obligation
Litigation	In the event of disputes arising from our debt collection process, we may process relevant personal data to facilitate the settlement, investigations, or legal proceedings for establishing, exercising, or defending legal claims.	Legitimate interest

Complaint resolution **Managing Data Subject Requests**	To address and resolve complaints or concerns raised by you. or third parties about our services, processes or processing of our personal data and to respond to data subject requests. To document the handling of complaints and requests from data subjects and to ensure the establishment, exercise or defence of legal claims.	Legal obligation Legitimate interest
Eligibility for payment solutions or discounts	By exception, in the context of our relationship and only based on your requests, we may process certain sensitive data relating to your health condition or special needs, in specific situations, in order to establish and document the eligibility criteria for special payment settlements or discounts.	Consent Legal obligation
Fraud prevention and incident investigation **Security monitoring**	We may process email, IT usage data, and logs to prevent fraudulent activities, unauthorized access, ensure security monitoring, and investigate and document security breaches, data breaches, or other incidents that may affect the security of your data. Personal. Protecting our business from fraud and maintaining the security of our business operations.	Legal obligation Legitimate interest
Research and development	Aggregated data for research and development purposes to improve our services and business and to improve our debt collection process.	Legitimate interest
Business Analytics & Reporting	Reviewing data for business analysis, reporting and performance evaluation, to monitor our debt collection process and business operations.	Legitimate interest
Evaluation and monitoring of service performance **Business Development**	To monitor and evaluate the quality of our services, to identify areas for improvement and improve the 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, internal policies and standards.	Legal obligation Legitimate interest
Risk management and control activities	To assess, manage, and control risks related to data security, privacy, and compliance, with the goal of ensuring 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 respecting your personal rights. Privacy Policy.
When we process personal data for our legitimate interests, we balance those interests with the rights and freedoms of the individuals whose data is processed. We take steps to ensure that your rights are protected. are also respected that personal data is processed in a fair and lawful manner.

3.3. CLIENTS - SPECIFIC INFORMATION ON THE DUE DILIGENCE PROCESS (SANCTIONS AND PEP VERIFICATION)

Purposes and legal bases of the examination

We conduct a sanctions and politically exposed persons (PEP) screening process as part of our commitment to comply with applicable laws and regulations governing international sanctions, anti-bribery and anti-corruption (ABC) measures, financial crime prevention, know-your-customer (KYC) requirements, anti-money laundering (AML) regulations, and countering the financing of terrorism (CTF) obligations. This screening process is essential for identifying and assessing potential risks associated with individuals or entities involved in our business relationships or financial transactions.

Sanctions and PEP screening serve several vital purposes, including:

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

We carry out the sanctions screening and PEP process in accordance with the General Data Protection Regulation ("GDPR") on the legal grounds set out in Article 6(1[1])(f) or Article 9(2)(e) and (f).[2]
These legal bases allow us to process your personal data. (i) when necessary to comply with our legal obligations, and (ii) when necessary for our legitimate interests, such as operating our business securely, protecting the integrity of our systems, operations, customers, business relationships, and users, detecting or preventing fraud, and pursuing other legitimate interests.

Collection of personal data, categories of data subjects and data sources

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

- **OUR CLIENTS:** This category includes personal data such as full names, contact details, dates of birth, gender, nationalities, citizenships, countries of residence, client IDs, and other pertinent information. In addition,

[1] According to art. **6 para. 1 lit. c) and f) of the GDPR:** "*The processing is lawful only if and to the extent that at least one of the following applies: (...) c) the processing is necessary for compliance with a legal obligation incumbent on the controller*. (...); *f) The processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, unless the interests or fundamental rights and freedoms of the data subject, which require the protection of personal data, prevail, in particular where the data subject is a child. (...)*".
[2] According to art. **9 para. 2 letters e) and f) of the GDPR:** "*(1) The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, health data or data concerning the sex life or sexual orientation of a natural person is prohibited. (2) Paragraph 1 shall not apply if one of the following conditions applies: (...) e) the processing relates to personal data that are manifestly made public by the data subject; f) the processing is necessary for the establishment, exercise or defense of a right in court or whenever the courts act in their judicial capacity. (...)*"

commercial and financial data necessary for effective examination may be collected. We obtain this data directly from data subjects during our debt collection process or indirectly from publicly available sources**.**

- **Persons included in the sanctions and PEP lists:** This group comprises the persons listed on the relevant sanctions and PEP lists. The data processed for screening may include full names, dates of birth, gender, citizenships, citizenships, countries of residence, other identifying information available in official public sources, contact details, positions or professions, details of sanctions and other relevant information available to the public. We obtain this data from authorized databases, third-party screening providers, publicly available information, regulators, law enforcement agencies, international organizations, and commercially available PEP databases.

Please note that we have no control over the information contained in public official records and datasets collected by third-party screening service providers. This data is collected from various sources and decisions on the disclosure of personal information lie with the relevant public bodies, balancing the public interest in disclosure and individuals' privacy rights.

Selection criteria and possible consequences in the event of a positive outcome

- **Selection criteria**. During the screening process, we use advanced and secure technologies and algorithms to compare personal data, such as name, dates of birth, nationalities and other essential information, with the relevant sanctions and PEP lists. This process is automated, but it requires human intervention for further analysis and investigation in cases of positive matches. No automated individual decision-making applies.

- **Consequences in case of a match.** If a positive match is detected during screening, it may trigger additional precautionary measures, such as increased monitoring or further investigations, as required by applicable laws and regulations. Our commitment is to handle such situations in full compliance with legal requirements, while protecting the confidentiality and integrity of personal data.

Data retention

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

- **Customers:** the data is actively processed as long as the debt collection process is ongoing and stored only for a maximum of 5 years, after the debt is fully repaid/closed or after the completion of all legal enforcement procedures.
- **Individuals on sanctions lists and PEPs from selected data sources:** data is actively processed during each screening session and then automatically removed; data resulting in potential matches is actively processed during manual review and analysis and stored only for a maximum period of 5 years after the end of the business relationship with the relevant customer.

Data sharing

In some cases, we may be required to disclose personal data to regulators, law enforcement agencies, or other authorized entities as part of our legal obligations or to fulfill our legitimate interests. We do not share personal data with third parties for marketing purposes.
To find out more about your rights about your personal data. and how to use them, please check the relevant section "Your rights" of this privacy policy.

3.4. CLIENTS - SERVICES AND TOOLS OFFERED BY THIRD PARTIES

While managing our debt collection process, we may use various tools and services offered by third parties to improve 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 can encompass a diverse range of functionality and solutions, including customer relationship management (CRM) systems, cloud solutions, email platforms, and other similar tools. These technologies allow us to collaborate effectively while complying with data security standards.

The use of these tools and services offered by third parties may require the sharing of certain categories of personal data relating to our customers. The types of data shared may vary depending on the specific tool or service used, but may include information necessary for the debt management business.

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

3.5. CUSTOMERS - HOW LONG DO WE KEEP YOUR DATA?

The retention period of your personal data varies depending on the stated processing purposes, as follows:

- 5 years from the date of debt settlement, according to consumer protection legislation
- 5 or 10 years from the end of the financial year during which the last supporting documents for the payment of the debt were prepared, in accordance with the Accounting Law no. 82/1991 and other accounting regulations issued in its application;
- 3 years from the date of communication of the response to the last request addressed by you to B2KPM, in accordance with the general limitation period of 3 years provided by the provisions of art. 2.517 of the Civil Code in which the right of action of any of the parties in relation to these communications may be prescribed.
- 10 years pursuant to the provisions of Article 11 paragraph 3 of GEO 15/2024 on loan administrators, as follows:
    - relevant correspondence with both the loan buyer and the borrower
    - the relevant instructions received from the credit buyer for the creditor's rights arising from each credit agreement or for the credit agreement itself, which it manages and executes on behalf of the credit buyer concerned;
    - the credit management agreement

3.6. CUSTOMERS - AUTOMATED DECISION-MAKING AND PROFILING

Automated decision-making: We do not engage in automated decision-making processes that produce significant legal effects or similar significant consequences for individuals based solely on automated processing. Rest assured that your rights and interests are not met. are protected by our manual review and human intervention in decision-making processes.

Profiling: We use profiling techniques in different contexts to optimize our operations, increase efficiency, and tailor our services to better meet your needs. Below are the main profiling activities we carry out, together with the respective reasoning and guarantees:

- **Debt portfolio performance analysis techniques** involve analyzing 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 data-driven decision-making to improve debt collection services. The consequences include improved debt collection strategies, improved services, and more efficient debt resolution processes.
- **The analysis of the efficiency of the debt collection process** involves techniques designed to streamline the debt collection process by analyzing the relevant data. Its purpose is to reduce errors and increase the overall efficiency of debt collection. It helps to facilitate the debt collection process and without errors. The consequences include a more efficient and efficient debt collection process, which leads to reduced delays and errors.
- **Identifying patterns of payment behavior** involves analyzing data to identify patterns of borrowers' payment behavior. It is used to adapt debt collection strategies based on observed payment patterns. The information obtained helps to personalize debt collection approaches. The result of such profiling includes more efficient and tailored debt collection services, aligned with the needs of our clients.
- **The analysis for the initiation of enforcement proceedings** is based on profiling techniques that provide relevant information to support the decision-making process on the initiation of legal enforcement proceedings and the most appropriate approach according to the specific details of the debt. The aim is to ensure compliance with legal requirements when initiating legal actions and to identify the most appropriate solutions for the managed receivables. Profiling helps to make informed decisions about the necessity and appropriateness of legal enforcement proceedings, including the enforcement of bailiffs. Human intervention is an integral part of this decision-making process, ensuring oversight and accountability, ensuring that all judicial proceedings are conducted accurately and in accordance with regulatory guidelines.
- **Security risk profiling** involves analyzing 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. Thanks to this profiling, you can expect improved 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** used to assess and manage customer-related risks, covering financial stability, reputational issues, compliance history, certifications, licenses, permits, conflicts of interest, integrity due diligence, and fraud prevention. It helps assess and manage 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. The results of profiling are reviewed through human intervention to ensure alignment with ethical standards and regulatory requirements.

In all profiling contexts, the overall 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 objectives. They increase security by identifying potential risks and vulnerabilities, ensure compliance with regulatory requirements, streamline processes to increase the efficiency of debt collection and enable personalized interactions tailored to customer preferences. The expected consequences are consistently positive, resulting in improved data security, strengthened compliance, optimized operational efficiency, and a more personalized and satisfying experience for our customers, ultimately contributing to successful debt management outcomes for both parties.

We assure you that all profiling activities are carried out in accordance with the relevant data protection laws and regulations. You have the right to object to profiling processes, if applicable.
If you have any concerns or questions about automated decision-making or profiling in our company, please do not hesitate to contact us using the contact details provided in the **"Contact Us" section** of this privacy policy.

3.7. WHO DO WE SHARE YOUR DATA WITH?

Sometimes, it is necessary for us to share your personal data. To fulfill our legal and contractual obligations and pursue our legitimate interests, we may share data with our affiliates, subsidiaries, or service providers to facilitate our business activity.

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

Service providers	These are companies that help us manage our business, including technical support, email hosting, cloud solutions, security and risk management tools, data analytics, and IT services. These partners are contractually bound to comply with our data privacy and security requirements, ensuring the protection of your personal information. Personal. They are authorized to access personal data only for the purposes we specify, contributing to the efficiency and security of our services.
Professional advisors	We may work with lawyers, accountants, auditors or consultants who may have access to your personal 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 are going through a merger, asset sale or significant organizational change, your data will be can be transferred to the new entity or owners.
Third-party tools and platforms	We use various third-party tools and platforms to improve our processes. These tools may process your email data on our behalf.
Other authorized recipients	There may be other authorized recipients with whom we need to share the data, depending on specific situations and laws,

We take steps to ensure the security and privacy of your personal data. when shared

3.8. International data transfers

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

- **Adequacy decisions** : If the European Commission declares that a country has good data protection, we may send data there without additional 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. Within this framework, your personal data will be may be transferred to participating U.S. companies without the need for additional collateral.
- **Standard Contractual Clauses**: We may use these approved contracts to ensure that your data is secure when outside the EEA.

Information about transfers can be obtained through the "Contact Us" section of the Privacy Policy.

3.9. How do we protect your data?

In the course of our business, we are dedicated to ensuring the security of your personal data. Personal. We use a range of technical and organizational measures to maintain the integrity and confidentiality of your information. protecting them against unauthorized access, disclosure, loss, alteration, or destruction.

Organisational safeguards	We have implemented various organizational measures, including policies, procedures, and guidelines that govern data protection practices within 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 protect your personal data during transmission and storage, making it impervious to unauthorized access or interception.
Access controls	Strict access controls to ensure that only authorized personnel have access to your data. Personal. Access privileges are granted on a need-to-know basis and are reviewed and updated regularly.
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	From the beginning, we integrate data protection into our processes, using privacy-enhancing technologies and practices to maintain 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, in accordance with the applicable regulations.
Periodic evaluations	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.
Others	Other security measures necessary to manage the privacy, availability and integrity of data, aligned with the development of technology.

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

3.10. Your rights

We are committed to ensuring transparency and ensuring that your rights are met. data subject are accessible and free of:

The right to withdraw your consent at any time	You can withdraw your consent to 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 being used. are collected and processed. This includes knowing the purposes of the processing, who is processing your data, and who is processing your data. and how long they will be kept.
Right to object to processing	When we process your personal data. on the basis of public or legitimate interest, you can object.
Right of access to your data	You can find out whether we are processing your data, obtain details of the processing and a copy of your data.
Right to rectify your data	You have the right to ensure that your data is not subject to any are correct and ask for corrections if necessary.
The right to restrict the processing of your personal data	You have the right, under certain circumstances, to restrict the processing of your personal data. In this case, we will not process the data for any purpose other than storing it.
The right to delete your data or otherwise remove it	You have the right, in certain circumstances, to obtain the deletion of your personal data.
The right to portability of your data	You can receive your personal data. in a structured, machine-readable format and, if possible, you can send them to another operator. This right applies when your personal data is not applicable. are processed automatically, based on your consent, a contract or pre-contractual obligations.
The right not to be subject to profiling and automated decision-making	You have the right not to be subject exclusively to automated decision-making processes, including profiling, which significantly affect you. This means that important decisions, such as those related to your rights, benefits, or issues. should not be taken exclusively by automated systems without human intervention. This right provides protection against unfair or discriminatory automated decisions.

Right to lodge a complaint	You have the right to file an action before the Romanian Supervisory Authority at the address: 28-30 G-ral Gheorghe Magheru Blvd., sector 1, postal code 010336, Bucharest, Romania, phone:+40318059211; email:anspdcp@dataprotection.ro or on the page web: http://www.dataprotection.ro/ or directly at the court.

Limitations or exceptions to the rights of data subjects:
While we respect your rights, legal or legitimate reasons may prevent us from fulfilling some requests. For example, if it conflicts with our legal obligations or the rights of others. We'll explain why if we can't fulfill your request.

Withdrawal of consent
You can withdraw your consent at any time. To do this:

- **Opt-out:** For non-essential cookies, adjust the settings on your device or browser. Cookies that are essential for security will still be active.

Withdrawing consent may affect your experience:

- If you withdraw your consent to 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.

The withdrawal of consent does not affect the lawfulness of any processing that took place prior to your withdrawal. We are committed to respecting your privacy choices and preferences.

To request any action regarding your rights, please contact us by email at privacy@b2kapital.ro or by post at our head office. Our Data Protection Officer (DPO) will assist you and respond to you as soon as possible, no later than three months.

4. BUSINESS PARTNER PRIVACY POLICY

This Privacy Policy generally applies to all of our existing and prospective business partners, including:

- Clients
- Investors
- Suppliers
- Suppliers
- External advisors
- Any third party involved in a business relationship with us.

Content of the Business Partner Privacy Policy

5.1. BUSINESS PARTNERS - WHAT INFORMATION DO WE COLLECT AND HOW?

How is the data collected?

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

- If you choose to share information about others, please note that you are responsible for any personal data of third parties obtained and shared, and you confirm the third party's consent to provide such data to us. **Direct collection** includes information you provide, such as data shared directly by you during the 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 such as professional social media profiles, business websites, or public records, if such information is relevant to the management of our business relationships.

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, ensuring appropriate safeguards.

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

Identifying Information	Name, contact details (such as telephone and postal addresses) and any other identifying information shared during the business relationship and relevant to our cooperation.
Professional and business information	Job titles, company names, industry affiliations, professional qualifications, and business contact information.
Correspondence records	Records of email correspondence, 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, records of financial transactions, including bank account details, credit ratings, payment terms, financial transactions, billing history, invoices related to professional agreements, order history and details of products or services, and other financial data relevant to our collaborations.

Sanctions verification data	Information on the verification of business partners against sanctions lists and databases of politically exposed persons, which may include sensitive data related to political opinions, criminal convictions or fraudulent activities *(please check the details in the next two sections).*
KYC and AML data	Data resulting from Know Your Customer (KYC) and Anti-Money Laundering (AML) checks and assessments performed on business partners to detect and prevent money laundering activities.
Potential data Conflicts of interest	Data relating 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, taking into account factors such as financial stability, reputation and compliance history.
Regulatory data	Data relating 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 relating to the performance and quality of services of our business partners, including service level agreements, performance evaluations and feedback.
Representatives' data	Data of employees or representatives of business partners, such as names, positions, contact details and other information relevant to the management of business relationships.
Insurance data	Information about insurance coverage and liability agreements between our company and business partners.
Marketing Preferences	Preferences for marketing communications, feedback, survey results, and other marketing-related data shared during our interactions.
Litigation	Information related to any legal disputes or complaints that may arise during our collaborations.
Audit Data and Compliance	Data relating to audits, assessments or inspections carried out by/or in relation to business partners to ensure compliance and quality.
Access rights and permission data	Data about the access rights and permissions granted to our business partners for various IT systems, applications and resources within our company.
Technical data	Technical information, such as system and application access logs, IP addresses, and the use 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 IT infrastructure, such as laptops, smartphones, or tablets.
Metadata logs and IT usage data	We may collect metadata logs and information related to IT usage across different systems and applications. This data plays an important role in investigating and documenting incidents, verifying the authenticity of

	communications, and maintaining security measures. It can include various elements, including timestamps, user identifiers, system activity records, access logs, IP addresses, device details, application usage logs, server logs, cloud data, and metadata associated with various interactions. In addition, this information helps monitor security and respond to incidents across our IT infrastructure, including but not limited to email systems, cloud environments, and other applications and software platforms integrated into our business operations.
Other relevant data	Depending on your interactions, we may process additional personal data, such as information related to our professional agreements, project details, information about events or contractual terms, and any other data relevant to our professional relationship.
Sensitive data	By exception, in the context of our relationships with our business partners, sensitive data is only processed in specific situations, which include the sanctions verification process, where we may collect and process sensitive data related to criminal convictions, fraudulent activities or politically exposed person (PEP) status (if such information is disclosed in public official lists) as part of our sanctions verification procedures to ensure regulatory requirements and to mitigate potential risks associated with individuals or entities. It is important to note that the processing of sensitive data is carried out with the utmost care and in strict accordance with applicable data protection laws. Our primary goal is to protect the rights and freedoms of individuals while fulfilling our legal obligations and maintaining the highest ethical standards in our professional relationships.

Obligation to provide personal data in the recruitment process

We request certain personal data from our business partners to fulfill key purposes such as risk assessment, compliance checks and collaborations, The consequence of not providing such requested data may include limited opportunities for collaboration and impact on our business relationship:

- Failure to provide the necessary data may restrict access to certain services, projects or collaborations.
- The absence of critical data may constrain our ability to initiate or continue our business partnership.

We value the accuracy and reliability of data, ensuring transparency and ethical standards in our collaborations. We encourage business partners to provide the personal data necessary to facilitate effective risk assessments and mutually beneficial collaborations

5.2. BUSINESS PARTNERS - WHY WE USE YOUR PERSONAL INFORMATION AND HOW DO 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, together with the legal bases and categories of data processed for each purpose.

Purpose	Details of the purpose	Legal basis
Business relationship management	Establishing and maintaining business relationships with our business partners,	Performance of the contract or steps before concluding a contract.

	including communication, collaboration and contractual arrangements.	Legitimate interests to have efficient business operations and collaboration.
Billing and payments	Processing financial transactions, invoicing, payments, and related financial activities necessary for our collaborations.	Performance of the contract Tax and accounting legal obligations
Facilitating communication	Facilitating communication through various channels and correspondence between you and our organization.	Performance of the contract or taking steps to conclude a contract and/or Legitimate interest in communicating with you for business-related matters.
Answering your questions	We may process your personal data to respond to your questions, queries or requests.	Performance of the contract or taking steps to conclude a contract
Sending newsletters and updates	If you have given your consent, we may use your email address to send you newsletters, updates or promotional materials related to our services or products.	Consent (You have the right to withdraw it at any time).
Compliance with legal obligations	We may process your personal data. to comply with legal obligations, including record keeping, regulatory requirements, and responding to legal requests.	Legal obligation
Sanctions review and risk assessment	We may process your personal data. to verify Business Partners against sanctions lists and to assess risks related to their financial stability, reputation and compliance history.	Legal obligation Legitimate interest *(Please check the details below in the next section)*
Know Your Customer (KYC) and Anti-Money Laundering (AML)	We may process your personal data. to conduct due diligence and assessments on business partners to prevent money laundering and fraudulent activities.	Legal obligation Legitimate interest in preventing fraud and illicit activities.
Assessment of conflict of interest	To assess potential conflicts of interest between our company and its business partners to ensure transparency and ethical conduct.	Legitimate interest in maintaining transparency and ethical conduct in professional collaborations
Verification of regulatory requirements	To verify the necessary industry-specific certifications, licenses, permits, and qualifications obtained by our business partners.	Legal obligations related to regulatory requirements and certifications.
Intellectual property rights management	To manage intellectual property rights and agreements between our company and its business partners, such as patents, trademarks or copyrights.	Performance of the contract Legitimate interests related to the establishment, exercise or defense of legal claims.

Evaluation of service performance	To evaluate the performance and quality of our business partners' services, including service level agreements and feedback.	Legitimate interest in evaluating and improving the quality of services provided by business partners.
Marketing & 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).
Registration of disputes	In the event of disputes arising from our cooperation, we may process relevant personal data to facilitate legal settlement, investigations or proceedings.	Legitimate interests in establishing, exercising or defending legal claims
Complaint resolution **Managing Data Subject Requests**	To address and resolve complaints or concerns raised by you. or third parties about our services, processes or processing of our personal data and to respond to data subject requests.	Legal obligations to document and respond to complaints and requests from data subjects. Legitimate interests related to the establishment, exercise or defense of legal claims.
Fraud prevention and incident investigation **Security monitoring**	We may process email, IT usage data, and logs to prevent fraudulent activities, unauthorized access, ensure security monitoring, and investigate and document security breaches, data breaches, or other incidents that may affect the security of your data. Personal.	Legal obligations to investigate and document security incidents, and Legitimate interests in protecting our business from fraud and maintaining the security of email communications.
Research and development	We may use aggregated data for research and development purposes to improve our services and business.	Legitimate interests in improving our offerings and business
Business Analytics & Reporting	We can analyze data for business analysis, reporting, and performance evaluation.	Legitimate interests in monitoring and improving our business operations
Monitoring and improving services **Business Development**	We may process data to monitor the quality of our services, identify areas for improvement and improve the business, or identify potential business opportunities, collaborations or partnerships.	Legitimate interests in maintaining and improving our services and pursuing the growth and development of the business.
Internal audit **External audit** **compliance monitoring**	To conduct internal and external audits and ongoing compliance monitoring to ensure that our organization adheres to regulatory requirements, policies, and internal standards.	Legal obligation and/or Legitimate interests
Risk management and control activities	To assess, manage, and control data security, privacy, and compliance risks.	Legitimate interests in ensuring the risk management, sustainability and compliance of our operations.

Please note that the specific purposes and legal bases for processing may vary depending on the circumstances and your interactions. with us. We always ensure that personal data is processed in accordance with applicable data protection laws and respecting your personal rights. Privacy Policy.
When we process personal data for our legitimate interests, we balance those interests with the rights and freedoms of the individuals whose data is processed. We take steps to ensure that your rights are protected. are also respected that personal data is processed in a fair and lawful manner.

5.3. BUSINESS PARTNERS - SPECIFIC INFORMATION ON THE DUE DILIGENCE PROCESS (SANCTIONS AND PEP VERIFICATION)

Purposes and legal bases of the examination

We conduct a sanctions and politically exposed persons (PEP) screening process as part of our commitment to comply with applicable laws and regulations governing international sanctions, anti-bribery and anti-corruption (ABC) measures, financial crime prevention, know-your-customer (KYC) requirements, anti-money laundering (AML) regulations, and countering the financing of terrorism (CTF) obligations. This screening process is essential for identifying and assessing potential risks associated with individuals or entities involved in our business relationships or financial transactions.

Sanctions and PEP screening serve several vital purposes, including:

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

We carry out the sanctions screening and PEP process in accordance with the General Data Protection Regulation ("GDPR") on the legal grounds set out in Article 6(1[3])(f) or Article 9(2)(e) and (f).[4]
These legal bases allow us to process your personal data. (i) when necessary to comply with our legal obligations, and (ii) when necessary for our legitimate interests, such as operating our business securely, protecting the integrity of our systems, operations, customers, business relationships, and users, detecting or preventing fraud, and pursuing other legitimate interests.

Collection of personal data, categories of data subjects and data sources

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

[3] According to art. **6 para. 1 lit. c) and f) of the GDPR:** "*The processing is lawful only if and to the extent that at least one of the following applies: (...) c) the processing is necessary for compliance with a legal obligation incumbent on the controller*. (...); *f) The processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, unless the interests or fundamental rights and freedoms of the data subject, which require the protection of personal data, prevail, in particular where the data subject is a child. (...)".*
[4] According to art. **9 para. 2 letters e) and f) of the GDPR:** "*(1) The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, health data or data concerning the sex life or sexual orientation of a natural person is prohibited. (2) Paragraph 1 shall not apply if one of the following conditions applies: (...) e) the processing relates to personal data that are manifestly made public by the data subject; f) the processing is necessary for the establishment, exercise or defense of a right in court or whenever the courts act in their judicial capacity. (...)"*

- **Our Business Partners:** This category includes personal data such as full names, contact details, dates of birth, gender, nationalities, nationalities, countries of residence, customer IDs, and other pertinent information. In addition, commercial and financial data necessary for effective examination may be collected. We obtain this data directly from data subjects in the course of our business relationships or indirectly from publicly available sources**.**
- **Persons included in the sanctions and PEP lists:** This group comprises the persons listed on the relevant sanctions and PEP lists. The data processed for screening may include full names, dates of birth, gender, citizenships, citizenships, countries of residence, other identifying information available in official public sources, contact details, positions or professions, details of sanctions and other relevant information available to the public. We obtain this data from authorized databases, third-party screening providers, publicly available information, regulators, law enforcement agencies, international organizations, and commercially available PEP databases.

Please note that we have no control over the information contained in public official records and datasets collected by third-party screening service providers. This data is collected from various sources and decisions on the disclosure of personal information lie with the relevant public bodies, balancing the public interest in disclosure and individuals' privacy rights.

Selection criteria and possible consequences in the event of a positive outcome

- **Selection criteria**. During the screening process, we use advanced and secure technologies and algorithms to compare personal data, such as name, dates of birth, nationalities and other essential information, with the relevant sanctions and PEP lists. This process is automated, but it requires human intervention for further analysis and investigation in cases of positive matches. No automated individual decision-making applies.
- **The consequences of a match.** If a positive match is detected during screening, it may trigger additional precautionary measures, such as increased monitoring or further investigations, as required by applicable laws and regulations. Our commitment is to handle such situations in full compliance with legal requirements, while protecting the confidentiality and integrity of personal data.

Data retention

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

- **Business partners:** the data is actively processed during the business relationship and stored only for a maximum of 5 years after the conclusion of the business contract.
- **Individuals on sanctions lists and PEPs from selected data sources:** data is actively processed during each screening session and then automatically removed; data resulting in potential matches is actively processed during manual review and analysis and stored only for a maximum period of 5 years after the end of the business relationship with the relevant business partner.

Data sharing

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

To find out more about your rights about your personal data. and how to use them, please check the relevant section "Your rights" of this privacy policy.

5.4. BUSINESS PARTNERS - SERVICES AND TOOLS OFFERED BY THIRD PARTIES

While managing our business relationships with our partners, we may use various tools and services offered by third parties to improve 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 tools and services offered by third parties 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 used, but may include information necessary for our professional collaborations.

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

5.5. BUSINESS PARTNERS - HOW LONG DO WE KEEP YOUR DATA?

We keep your personal data. for as long as necessary for the execution and management of our contractual relationship and up to 5 years after the end of the contractual relationship or for a longer period if other legal deadlines apply.
We always ensure compliance with the relevant legal obligations and adjust our retention periods accordingly to meet these requirements. Our primary purpose is to retain data for as long as necessary to fulfill the purposes outlined in this privacy policy and to comply with any legal obligations.
The time we keep can change depending on things like:

- Type of data – Some data requires longer retention than others.
- The purposes for which we process your personal data.
- Legal and regulatory requirements. Sometimes the law says that we need to keep the data for certain periods.
- Our business needs and operational requirements affect how long we retain data.

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

5.6. BUSINESS PARTNERS - AUTOMATED DECISION-MAKING AND PROFILING

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

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

- **Security risk profiling** involves analyzing 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. Thanks to this profiling, you can expect improved security measures to protect your data and the systems you interact with, leading to a safer and more secure cooperative environment.
- **Risk assessment and due diligence profiling techniques are** used 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 assess and manage 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 evaluate the performance and quality of our business partners' services by analyzing performance indicators, service level agreements, and feedback data. This helps to evaluate and increase the efficiency and effectiveness of our cooperation. The consequences include better quality of service and more efficient interactions, tailored to meet both of our needs.

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

We assure you that any profiling activities are carried out in accordance with the relevant data protection laws and regulations. You have the right to object to profiling processes, if applicable.
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.

5.7. WHO DO WE SHARE YOUR DATA WITH?

Sometimes, it is necessary for us to share your personal data. To fulfill our legal and contractual obligations and pursue our legitimate interests, we may share data with our affiliates, subsidiaries, or service providers to facilitate our business activity.

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

Service providers	These are companies that help us manage our business, including technical support, email hosting, cloud solutions, security and risk management tools, data analytics, and IT services. These partners are contractually bound to comply with our data privacy and security requirements, ensuring the protection of your personal information. Personal. They are authorized to access personal data only

	for the purposes we specify, contributing to the efficiency and security of our services.
Professional advisors	We may work with lawyers, accountants, auditors or consultants who may have access to your personal 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 are going through a merger, asset sale or significant organizational change, your data will be can be transferred to the new entity or owners.
Third-party tools and platforms	We use various third-party tools and platforms to improve our processes. These tools may process your email data on our behalf.
Other authorized recipients	There may be other authorized recipients with whom we need to share the data, depending on specific situations and laws,

We take steps to ensure the security and privacy of your personal data. when shared

5.8. International data transfers

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

- **Adequacy decisions** : If the European Commission declares that a country has good data protection, we may send data there without additional 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. Within this framework, your personal data will be may be transferred to participating U.S. companies without the need for additional collateral.
- **Standard Contractual Clauses**: We may use these approved contracts to ensure that your data is secure when outside the EEA.

Information about transfers can be obtained through the "Contact Us" section of the Privacy Policy.

5.9. How do we protect your data?

In the course of our business, we are dedicated to ensuring the security of your personal data. Personal. We use a range of technical and organizational measures to maintain the integrity and confidentiality of your information. protecting them against unauthorized access, disclosure, loss, alteration, or destruction.

Organisational safeguards	We have implemented various organizational measures, including policies, procedures, and guidelines that govern data protection practices within 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 protect your personal data during transmission and storage, making it impervious to unauthorized access or interception.

Access controls	Strict access controls are firmly in place to ensure that only authorized personnel have access to your personal data. Personal. Access privileges are granted on a need-to-know basis and are reviewed and updated regularly.
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	From the beginning, we integrate data protection into our processes, using privacy-enhancing technologies and practices to maintain 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, in accordance with the applicable regulations.
Periodic evaluations	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.
Others	Other security measures necessary to manage the privacy, availability and integrity of data, aligned with the development of technology.

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

5.10. Your rights

We are committed to ensuring transparency and ensuring that your rights are met. data subject are accessible and free of:

The right to withdraw your consent at any time	You can withdraw your consent to 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 being used. are collected and processed. This includes knowing the purposes of the processing, who is processing your data, and who is processing your data. and how long they will be kept.
Right to object to processing	When we process your personal data. on the basis of public or legitimate interest, you can object.
Right of access to your data	You can find out whether we are processing your data, obtain details of the processing and a copy of your data.
Right to rectify your data	You have the right to ensure that your data is not subject to any are correct and ask for corrections if necessary.

The right to restrict the processing of your personal data	You have the right, under certain circumstances, to restrict the processing of your personal data. In this case, we will not process the data for any purpose other than storing it.
The right to delete your data or otherwise remove it	You have the right, in certain circumstances, to obtain the deletion of your personal data.
The right to portability of your data	You can receive your personal data. in a structured, machine-readable format and, if possible, you can send them to another operator. This right applies when your personal data is not applicable. are processed automatically, based on your consent, a contract or pre-contractual obligations.
The right not to be subject to profiling and automated decision-making	You have the right not to be subject exclusively to automated decision-making processes, including profiling, which significantly affect you. This means that important decisions, such as those related to your rights, benefits, or issues. should not be taken exclusively by automated systems without human intervention. This right provides protection against unfair or discriminatory automated decisions.
Right to lodge a complaint	You have the right to file a complaint with the Romanian Supervisory Authority at the address: 28-30 G-ral Gheorghe Magheru Blvd., sector 1, postal code 010336, Bucharest, Romania, telefon:+40318059211;email:anspdcp@dataprotection.ro, on the website: http://www.dataprotection.ro/sau directly to the court.

Limitations or exceptions to the rights of data subjects:
While we respect your rights, legal or legitimate reasons may prevent us from fulfilling some requests. For example, if it conflicts with our legal obligations or the rights of others. We'll explain why if we can't fulfill your request.

Withdrawal of consent
You can withdraw your consent at any time. To do this:

- **Opt-out:** For non-essential cookies, adjust the settings on your device or browser. Cookies that are essential for security will still be active.

Withdrawing consent may affect your experience:

- If you withdraw your consent to 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.

The withdrawal of consent does not affect the lawfulness of any processing that took place prior to your withdrawal. We are committed to respecting your privacy choices and preferences.

To request any action regarding your rights, please contact us by email at dpo@veraltis.ro or by post at our head office. Our Data Protection Officer (DPO) will assist you and respond to you as soon as possible, no later than three months.

6. RECRUITMENT PRIVACY POLICY

6.1. TO WHOM THIS PRIVACY POLICY APPLIES

This **recruitment privacy policy** applies to all individuals who interact with us during the recruitment and employment process. This includes, but is not limited to, job seekers, candidates and potential employees seeking employment opportunities within the Company.
The Company processes your personal data. For the purpose of recruiting, processing and evaluating your application. for a position within the Company

For some processing activities, the Company and any of the Company's affiliates may process your personal data in a common control relationship, where, for the position level, your request should be evaluated by any of the groups of companies.tag.

By submitting your personal information. and your involvement in our recruitment process, you agree to the practices outlined in this policy.

Please take the time to carefully review this policy to understand how we collect, use, and protect your personal data. Personal. If you have any questions or concerns about this policy or our data handling practices, please feel free to contact us using the information provided in this document.

6.2. WHAT INFORMATION DO WE COLLECT AND HOW?

How is the data collected?

We collect personal data through various means to facilitate our professional interactions and collaborations and to ensure security.
If you choose to share information about others, please note that you are responsible for any personal data of third parties obtained and shared through the email exchange process and confirm the third party's consent to provide such data to us.

- **Direct collection** includes information you provide, such as data shared directly by you during the recruitment process and professional interactions, such as your name, contact details, professional information, and other relevant documents or information.
- **Indirect collection from accepted third parties.** We may collect information about you from third parties, such as your former employers, when you give your consent to check your professional references.

- **Indirect collection from publicly available sources.** We may collect publicly available information about you from sources such as professional social media profiles, business websites, or public records, if such information is relevant to our recruitment process.

What categories of data are processed?

During our recruitment process, we may process personal data necessary for the recruitment and employment process. The specific personal data collected may vary depending on the nature of the position you are applying for and the particular requirements applicable to the position you are considering. We are committed to handling all data with care and in accordance with applicable data protection laws and regulations, ensuring appropriate safeguards.

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

Identifying Information	This category comprises personal information such as your first name, last name, date of birth, home address, residence, nationality, nationality, nationality, identity card or passport data (e.g. CNP, ID card/passport series and number) or other identifying data included in your CV. and/or any recruitment-related forms.
Contact details	This includes your mailing address, phone number, and email address.
Signature and photo	Information included in documents provided during the recruitment process, such as signature and photo.
Demographics	We may collect data about your age, gender, etc. and, if required for certain positions, the existence or type of driving licence.
Work Experience Data	Information relating to your occupation/profession, the nature of the activities involved, your previous place of employment, including periods of employment, job functions, names and addresses of previous employers, details of your significant projects and achievements in your professional history.
Educational data and professional certifications	Details of studies, such as the name and type of studies completed, educational institutions attended (schools and universities), duration, specialization, diplomas, studies, certifications, and participation in training programs and conferences.
Data on professional skills and competences	Information about the foreign languages you know or use and knowledge of computer use, as mentioned in your CV.
Remuneration data, Taxes and taxes	Details of the salary or remuneration requested, bonuses, benefits and data on applicable taxes and fees according to tax legislation.
Communication Recordings	Records of email correspondence, meeting minutes, call logs, and other communication-related data exchanged during our professional interactions, such as text, attachments, documents, images, and any other information shared during our correspondence, including communication with recruitment companies or former employers, as part of the recruitment process.
Data from video recording (image and voice)	Only in limited cases where video recordings are made during online interviews, only on the basis of your consent.

Candidate evaluation data	This category comprises opinions and resolutions of authorized personnel involved in the recruitment process, references, interview notes, records/results of pre-employment checks, and more.
References obtained from former employers	Details of your professional activities and duration of employment obtained from your former employers, based on your consent.
Potential data Conflicts of interest	Information about the existence of family or affinity relationships with employees or persons in the management of our company, group companies, our business partners, etc.
Regulatory data	Data relating to regulatory requirements, certifications, licenses, permits, accreditations, and industry-specific qualifications obtained by you. and necessary for the position for which you applied.
Disputes/complaints Data Subject Requests	Information regarding any complaints, data subject requests, and legal disputes that may arise during our recruitment process.
Audit Data and Compliance	Data relating to audits, assessments or inspections carried out by/or related to the recruitment process to ensure compliance and quality.
Communication metadata Logs and IT usage data	To investigate and document incidents, check phishing emails, and maintain security, we may collect logs and other IT usage data related to our communications. This data may include timestamps, email addresses, and subject lines related to our email communications, server logs, IP addresses, device information, email delivery logs, metadata related to email exchanges, and information for security monitoring and incident response.
Other relevant data	Any additional personal data voluntarily provided by you during interviews and correspondence to respond to specific requests or questions.
Sensitive data	By exception, in the context of our recruitment process, sensitive data is only processed in specific situations, when it is necessary for the fulfilment of the recruitment process or is necessary for certain executive functions. The sensitive data we may process includes: ▪ **Health data related to occupational medicine**: Information about certain special medical conditions or details about possible disabilities, including work restrictions and/or special requirements. For selected candidates, health data related to occupational medicine and assessment of work capacity. ▪ **Data on disciplinary sanctions: Data on disciplinary sanctions for which the limitation period has not expired.** ▪ **Data on restrictions/prohibitions on the exercise of certain professions**: applicable for certain functions. ▪ **Data on political and public exposure**: if applicable.

Obligation to provide personal data during the recruitment process

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

- Failure to provide the necessary data may restrict access to certain positions or jobs.
- The absence of critical data can constrain our ability to complete the recruitment process and initiate an employment relationship.

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

6.3. WHY WE USE YOUR PERSONAL INFORMATION AND HOW DO 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, together with the legal bases and categories of data processed for each purpose.

Purpose	Details of the purpose	Legal basis
Identification of eligible candidates	Identifying suitable candidates for this position.	Taking steps to conclude the employment contract. Legitimate interest in filling existing vacancies.
Conducting job interviews	Organizing and conducting job interviews.	Taking steps to conclude the employment contract.
Skills assessment	Analysis of candidates' profiles, both professional and personal.	Taking steps to conclude the employment contract Legitimate interest for an appropriate selection.
Legal conditions of verification	Ensuring that candidates meet the legal requirements for certain positions (certifications, licenses, permits, accreditations, and industry-specific qualifications).	Legal obligation
Facilitating communication	Facilitating communication through various channels and correspondence between you and our Company.	Taking steps to conclude your employment contract Legitimate interest in communicating with you for recruitment issues.
Obtaining references	Collecting references from former employers.	Consent (Can be withdrawn at any time)
Answering your questions	To respond to your questions, inquiries, or requests.	Taking steps to conclude the employment contract
Employment Documentation	Creation of the necessary employment-related documents.	Taking steps to conclude the employment contract
Retention of records and documentation	To respond to legal requests.	Legal obligation

	Keeping records and documents related to recruitment (in physical and/or electronic format).	Legitimate interest – demonstrate compliance and fairness of the process.
Assessment of conflict of interest	To assess potential conflicts of interest between our Company and candidates to ensure transparency and ethical conduct.	Legitimate interest in maintaining transparency and ethical conduct in professional collaborations
Maintaining candidate databases	Building and maintaining a database of potential candidates for future recruitment.	Consent (Can be withdrawn at any time)
Previous occupational medicine procedures	Assessing the health status and work capacity of the selected candidates.	Legal obligation
Interview committees / multi-interviewer evaluations	To facilitate the assessment process when multiple interviewers participate, ensuring the fairness and consistency of their assessments.	Consent (Can be withdrawn at any time) Legitimate interest in conducting a fair and efficient interview process
Determination of remuneration	To determine salary expectations, benefits, and tax-related information.	Taking steps to conclude the employment contract
Litigation	To facilitate the resolution, investigations or legal proceedings, in the event of any disputes arising.	Legitimate interests in establishing, exercising or defending legal claims
Complaint resolution Managing Data Subject Requests	To address and resolve complaints or concerns raised by you. or third parties about our services, processes or processing of our personal data and to respond to data subject requests.	Legal obligations to document and respond to complaints and requests from data subjects. Legitimate interests related to the establishment, exercise or defense of legal claims.
Fraud prevention and incident investigation Security monitoring	We may process email, IT usage data, and logs to prevent fraudulent activities, unauthorized access, ensure security monitoring, and investigate and document security breaches, data breaches, or other incidents that may affect the security of your data. Personal.	Legal obligations to investigate and document security incidents, and Legitimate interests in ensuring security and preventing fraud and illicit activities.
Research and development	We may use aggregated data for research and development purposes to improve our recruitment.	Legitimate interests in improving the business
Internal analysis and recruitment strategy	We can process data for analyzing and optimizing the recruitment process, developing recruitment strategies.	Legitimate interests in maintaining and improving our recruitment process and strategy.
Protecting the company's reputation and interests	Protecting the Company's reputation and interests, including prudent risk management	Legitimate interest in protecting reputation
Internal audit External audit	To conduct internal and external audits and ongoing compliance monitoring to ensure that	Legal obligation and/or Legitimate interests

Compliance monitoring	our organization adheres to regulatory requirements, policies, and internal standards.	
Risk management and control activities	To assess, manage, and control data security, privacy, and compliance risks.	Legitimate interests in ensuring the risk management, sustainability and compliance of our operations.
Processing of sensitive data	Processed only when necessary for specific situations or for executive functions, as required.	Legal obligation, if applicable Legitimate interest to demonstrate compliance, establishment, defense and enforcement of our rights in court.

Please note that the specific purposes and legal bases for processing your personal data are not subject to any of your personal data. may vary depending on the context and your commitment. to our recruitment process. We consistently comply with the relevant data protection regulations and support your privacy rights with the utmost care.
When we process personal data for our legitimate interests, we balance those interests with the rights and freedoms of the individuals whose data is processed. We take steps to ensure that your rights are protected. are also respected that personal data is processed in a fair and lawful manner.

6.4. HOW LONG DO WE KEEP YOUR DATA?

We keep your personal data. for as long as necessary for the execution of our recruitment process. We ensure compliance with the relevant legal obligations and adjust our retention periods accordingly to meet these requirements. Our primary purpose is to retain data for as long as necessary to fulfill the purposes outlined in this privacy policy and to comply with any legal obligations.
The time we keep can change depending on things like:

- Type of data – Some data requires longer retention than others.
- The purposes for which we process your personal data.
- Legal and regulatory requirements. Sometimes the law says that we need to keep the data for certain periods.
- Our business needs and operational requirements affect how long we retain data.

In the context of our recruitment process, personal data is usually retained for 6 months after the completion of the recruitment process, mainly for audit purposes. However, data may be retained beyond this initial period in the following circumstances:

- Based on the candidate's consent, the data may be kept for a duration of up to 3 years for subsequent recruitment opportunities.
- In case of security breaches, data security breaches or integrity incidents (integrity warning), the data may be kept for up to 3 years.
- The data may be retained for longer periods in response to requests from the authorities, in accordance with the law.
- In situations of litigation in court or ongoing litigation, data may be retained for 3 years after the settlement of the dispute or dispute.
- Following the exercise of the right to restriction of processing, the data may be kept until the end of the restriction period.

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

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

6.5. AUTOMATED DECISION-MAKING AND PROFILING

Automated decision-making: We do not engage in automated decision-making processes that produce significant legal effects or similar significant consequences for individuals based solely on automated processing. Our decision-making processes are based on human intervention and evaluation to ensure fairness and individual consideration.

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

- **Security risk profiling** involves analyzing 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. Thanks to this profiling, you can expect improved security measures to protect your data and the systems you interact with, leading to a safer and more secure environment.
- **Analysis of soft skills and personal skills:** We can apply soft profiling techniques to assess the soft skills and personal skills of candidates during the recruitment process. It is important to note that this profiling involves human intervention and evaluation, ensuring that assessments are done with care and consideration. Soft profiling of candidates allows us to obtain information about their soft skills and personal competencies, which are valuable for determining their suitability for specific roles. This assessment complements the traditional assessment process, providing a more comprehensive understanding of a candidate's qualifications and potential for fit within our company. Very importantly, human intervention in this profiling process ensures fairness and individualized consideration, improving the quality of our recruitment decisions.

In all profiling contexts, the logic is to provide enhanced security, compliance, efficiency, and effective interactions. The expected consequences are generally positive and aim to improve the overall experience and results for our professional relationships. We assure you that any profiling activities are carried out in accordance with the relevant data protection laws and regulations. You have the right to object to profiling processes, if applicable.

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

6.6. THIRD-PARTY SERVICES AND TOOLS

These third-party tools and services may encompass a variety of functionalities and solutions, enhancing our ability to work together efficiently and securely.
The use of these tools and services offered by third parties may require the sharing of certain categories of personal data relating to our candidates. The types of data shared may vary depending on the specific tool or service used, but may include information necessary for our recruitment process and professional cooperation.

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

6.7. WHO DO WE SHARE YOUR DATA WITH?

Sometimes, it is necessary for us to share your personal data. To fulfill our legal and contractual obligations and pursue our legitimate interests, we may share data with our affiliates, subsidiaries, or service providers to facilitate our business activity. We take steps to ensure the security and privacy of your personal data. when shared.

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

Companies in the B2 Impact Group	When for job level, your application should be evaluated by any of the Group of Companies. You can find the data of the companies in the Group here.
Service providers	These are companies that help us manage our business, including technical support, email hosting, cloud solutions, security and risk management tools, data analytics, and IT services. These partners are contractually bound to comply with our data privacy and security requirements, ensuring the protection of your personal information. Personal. They are authorized to access personal data only for the purposes we specify, contributing to the efficiency and security of our services.
Professional advisors	We may work with lawyers, accountants, auditors or consultants who may have access to your personal 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 are going through a merger, asset sale or significant organizational change, your data will be can be transferred to the new entity or owners.
Third-party tools and platforms	We use various third-party tools and platforms to improve our processes. These tools may process your email data on our behalf.
Other authorized recipients	There may be other authorized recipients with whom we need to share the data, depending on specific situations and laws,

6.8. INTERNATIONAL DATA TRANSFERS

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

- **Adequacy decisions** : If the European Commission declares that a country has good data protection, we may send data there without additional 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. Within this framework,

your personal data will be may be transferred to participating U.S. companies without the need for additional collateral.

- **Standard Contractual Clauses**: We may use these approved contracts to ensure that your data is secure when outside the EEA.

Information about transfers can be obtained through the "**Contact Us**" section of the Privacy Policy.

6.9. HOW DO WE PROTECT YOUR DATA?

In the course of our business, we are dedicated to ensuring the security of your personal data. Personal. We use a range of technical and organizational measures to maintain the integrity and confidentiality of your information. protecting them against unauthorized access, disclosure, loss, alteration, or destruction.

Organisational safeguards	We have implemented various organizational measures, including policies, procedures, and guidelines that govern data protection practices within 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 protect your personal data during transmission and storage, making it impervious to unauthorized access or interception.
Access controls	Strict access controls are firmly in place to ensure that only authorized personnel have access to your personal data. Personal. Access privileges are granted on a need-to-know basis and are reviewed and updated regularly.
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	From the beginning, we integrate data protection into our processes, using privacy-enhancing technologies and practices to maintain 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, in accordance with the applicable regulations.
Periodic evaluations	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.
Others	Other security measures necessary to manage the privacy, availability and integrity of data, aligned with the development of technology.

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

6.10. YOUR RIGHTS

We are committed to ensuring transparency and ensuring that your rights are met. data subject are accessible and free of:

The right to withdraw your consent at any time	You can withdraw your consent to 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 being used. are collected and processed. This includes knowing the purposes of the processing, who is processing your data, and who is processing your data. and how long they will be kept.
Right to object to processing	When we process your personal data. on the basis of public or legitimate interest, you can object.
Right of access to your data	You can find out whether we are processing your data, obtain details of the processing and a copy of your data.
Right to rectify your data	You have the right to ensure that your data is not subject to any are correct and ask for corrections if necessary.
The right to restrict the processing of your personal data	You have the right, under certain circumstances, to restrict the processing of your personal data. In this case, we will not process the data for any purpose other than storing it.
The right to delete your data or otherwise remove it	You have the right, in certain circumstances, to obtain the deletion of your personal data.
The right to portability of your data	You can receive your personal data. in a structured, machine-readable format and, if possible, you can send them to another operator. This right applies when your personal data is not applicable. are processed automatically, based on your consent, a contract or pre-contractual obligations.
The right not to be subject to profiling and automated decision-making	You have the right not to be subject exclusively to automated decision-making processes, including profiling, which significantly affect you. This means that important decisions, such as those related to your rights, benefits, or issues. should not be taken exclusively by automated systems without human intervention. This right provides protection against unfair or discriminatory automated decisions.
Right to lodge a complaint	You have the right to file an action before the Romanian Supervisory Authority at the address: 28-30 G-ral Gheorghe Magheru Blvd., sector 1, postal code 010336, Bucharest, Romania, phone:+40318059211; e-mail:anspdcp@dataprotection.ro, on page b: http://www.dataprotection.ro/ or directly at the court.

Limitations or exceptions to the rights of data subjects:
While we respect your rights, legal or legitimate reasons may prevent us from fulfilling some requests. For example, if it conflicts with our legal obligations or the rights of others. We'll explain why if we can't fulfill your request.

Withdrawal of consent

If you have given your consent for the specific purposes outlined in this privacy policy, you have the right to withdraw your consent at any time. To do this, please contact us immediately using the contact details provided in **the "Contact Us" section** or dedicated consent management tools, if available.

Please note that the withdrawal of consent does not affect the lawfulness of any processing that took place prior to your withdrawal. We are committed to respecting your privacy choices and preferences.

- **Obtaining references:** If you choose to withdraw your consent to obtain references, please be aware that doing so may limit our ability to obtain relevant information about your professional experience, which could affect our assessment of your suitability for a particular role. However, it will not affect your participation in our recruitment process or your eligibility. for other positions.
- **Interview committees/evaluations with multiple interviewers:** You have the right to withdraw your consent for the recording of the interview. However, please note that withdrawing consent may limit the effectiveness of the recruitment process. We may need to have multiple discussions and meetings, which could extend the time it takes to complete the assessment and assessment of candidates. This can also limit our ability to provide a comprehensive assessment in a single meeting, leading to additional discussion between interviewers.
- **Maintaining candidate databases:** If you decide to withdraw your consent to keep your data in our candidate database, we will promptly remove your information from our records. This means that we will no longer consider you for future recruitment opportunities and you may need to reapply if you want to be considered for new positions.

To request any action regarding your rights, please contact us by email at dpo@veraltis.ro or by post at our head office. Our Data Protection Officer (DPO) will assist you and respond to you as soon as possible, no later than three months.

7. 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 periodically check our Privacy Policy for the latest information about our privacy practices.

We are committed to keeping you informed of 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** of our website. This section provides a record of all previous versions, allowing you to review any changes made over time.

8. KEY LEGAL TERMS AND TECHNIQUES USED IN THE PRIVACY POLICY

Here are some definitions for key terms and legal concepts used in our Privacy Policy to ensure clarity. These definitions are intended 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 do not hesitate to contact us. Your understanding of your rights our data and practices is essential to us.

Personal data	Any information about you, such as your name, email address, or other identifying information that can directly or indirectly identify you as an individual.
Data processing	Actions taken on personal data, including but not limited to collection, storage, organization, modification, use, disclosure, or deletion.
Data processed	Specific personal data that we collect, use, or otherwise process in accordance with this Privacy Policy.
Data Controller	This is us; We are responsible for determining how and why data is processed and ensure compliance with data protection laws.
Data subject	An individual whose personal data is being processed. This term often refers to you, the user of our website or our business partner.
Consent	Your voluntary and informed consent to the processing of your data for specific purposes, obtained by clear and transparent means.
Legitimate interests	One of the legal grounds for processing personal data indicates that we have good grounds for processing data that do not compromise your rights or interests.
Profiling	Automated data processing for the purpose of analyzing and predicting behavior, preferences, or interests, often used to personalize user experiences, perform risk assessments, or for analytics.
Automated decision-making	Decisions made exclusively by machines or automated systems, without human intervention, which can affect the rights and freedoms of individuals.
Data Protection Officer (DPO)	A designated person responsible for overseeing data protection compliance within our organisation and acting as a point of contact for data-related questions.
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 cross-border data sharing outside the European Economic Area ("EEA"), which may require specific safeguards to ensure data protection.
Adequacy decisions	Official approvals indicating that certain countries outside the EEA offer an adequate level of data protection, allowing data transfers without additional safeguards.
Standard contract 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 consent (opt-in) or opt-out (opt-out) to certain data processing activities, such as subscribing or unsubscribing to our newsletters or for cookies and tracking technologies.
Cookies	Small chunks of data stored on your device to improve your web browsing experience, including tracking preferences and user behavior for various purposes.
Geographical position	Information about a user's approximate location, such as their country and city, often collected with the user's consent for location-based services.
Due diligence	The process of conducting research and assessments to assess the suitability and credibility of potential business partners, ensuring that they align with our business objectives and standards.

Rights of data subjects	Your rights legal information regarding your personal data. including the right to access, rectify, delete, restrict processing, object to processing and data portability.
Data encryption	The process of converting data into code or cipher to protect its privacy 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 persons.
Data minimization	The practice of collecting only the data necessary for the specified purposes of the processing, minimizing the amount of personal data collected.
Privacy by design and default	Establishing confidentiality as 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 personal data	Storing or using your data for certain periods when we store or use your data for specific purposes, in accordance with legal and regulatory requirements.
Purposes	Specific and transparent reasons for the processing of personal data, presented in this privacy policy or provided to you. when you obtain your consent.
Legal basis	Legal justification for the processing of personal data, ensuring that the processing aligns with applicable data protection laws.
Legal obligation	Processing of personal data due to applicable laws, regulations or legal obligations.