PRIVACY POLICY

1. Introduction:

1.1 Purpose and Scope

BerryPax ("we," "us," or "our") is committed to upholding the highest standards of data protection and privacy in accordance with applicable legal and regulatory requirements, including the General Data Protection Regulation ("GDPR"). This Privacy Policy outlines how BerryPax collects, processes, and protects personal data belonging to clients, prospective clients, suppliers, business partners, and employees.

Personal data processing is integral to our operations, including client relationship management, supplier engagement, contractual obligations, recruitment, personnel administration, and compliance with legal and regulatory obligations. Our commitment to privacy protection ensures that personal data is processed securely, lawfully, and transparently.

BerryPax has implemented comprehensive technical and organizational measures to ensure data security and compliance with regulatory requirements. We continuously monitor and audit our internal data protection policies and ensure that all employees strictly adhere to our internal data handling standards. Additionally, BerryPax undertakes periodic reviews of this Privacy Policy to reflect evolving legal obligations and industry best practices. Our data retention practices are governed by the latest retention policy, ensuring that personal data is not stored for longer than necessary.

This Privacy Policy, along with our established protocols, serves as the governing framework for all data processing activities at BerryPax.

1.2 Definition of Personal Data

For the purposes of this Privacy Policy, "personal data" refers to any information relating to an identified or identifiable natural person ("data subject"). A data subject is considered identifiable if they can be directly or indirectly identified through identifiers such as name, contact details, location data, identification numbers, or other personal attributes.

Personal data processed by BerryPax includes, but is not limited to, information related to:

- Clients and prospective clients
- Suppliers and business partners

- Employees and job applicants
- Other stakeholders interacting with BerryPax

1.3 Categories of Personal Data

BerryPax classifies personal data into two primary categories:

1. **Ordinary (Non-Sensitive) Personal Data**: This includes general information such as names, addresses, phone numbers, email addresses, employee IDs, job titles, and educational background. Certain types of non-sensitive data, such as financial information (income, wealth details), may be deemed confidential and subject to heightened security measures.
2. **Special Categories of Personal Data (Sensitive Data)**: In compliance with GDPR Article 9, sensitive data includes information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health information, and data concerning an individual's sex life or sexual orientation. Processing of such data requires explicit consent or a valid legal basis as outlined in Section 2.

In addition, any data related to criminal offences or national identification numbers (such as CPR numbers) are subject to specific legal provisions governing their processing.

1.4 Business Contact and Sole Proprietorship Data

While corporate or business-related information is generally not considered personal data, details concerning an individual's professional role—such as their name, job title, work email, and work phone number—are regarded as personal data. Additionally, for sole proprietors, any business-related data is also considered personal data since it pertains to an identifiable natural person.

1.5 Purpose of Processing Personal Data

BerryPax processes personal data for legitimate business purposes, including but not limited to:

- Managing client and supplier relationships
- Executing contracts and sales agreements
- Employee recruitment and administration
- Fulfilling legal and regulatory obligations
- Providing customer support and operational communications

All personal data processing activities are carried out in compliance with GDPR and other applicable regulations, ensuring that personal data is processed lawfully, fairly, and transparently.

1.6 Principles of Data Processing

BerryPax adheres to the following core data protection principles, in accordance with GDPR:

1. **Lawfulness, Fairness, and Transparency**: Personal data is processed in a lawful, fair, and transparent manner, ensuring that data subjects are informed about how their data is used.
2. **Purpose Limitation**: Personal data is collected for specific, explicit, and legitimate purposes and is not processed further in a manner that is incompatible with those purposes.
3. **Data Minimization**: We only collect personal data that is relevant and necessary for the intended processing purposes.
4. **Accuracy**: We ensure that personal data is accurate and up-to-date. Any inaccurate data is promptly rectified or deleted.
5. **Storage Limitation**: Personal data is retained only for as long as necessary to fulfill the purposes for which it was collected, in compliance with our data retention policy.
6. **Integrity and Confidentiality**: Personal data is processed securely with appropriate measures to prevent unauthorized access, unlawful processing, loss, destruction, or damage.

1.7 Accountability and Compliance

BerryPax takes full responsibility for ensuring compliance with these principles. Through our accountability framework, we demonstrate our commitment to GDPR compliance by implementing:

- Internal audits and monitoring mechanisms
- Ongoing staff training and awareness programs
- Clear assignment of responsibilities for data protection
- Continuous assessment and improvement of data protection policies

This Privacy Policy serves as a key document in reinforcing BerryPax's commitment to lawful and responsible personal data processing. All employees and stakeholders handling personal data must be familiar with and adhere to these principles.

---

2. Legal Basis for Processing Personal Data

2.1 In compliance with the General Data Protection Regulation (GDPR) and other applicable laws, all personal data processing activities conducted by BerryPax must be based on a valid legal basis. The appropriate legal basis depends on the nature and category of the personal data being processed.

For ordinary non-sensitive personal data, including names, addresses, email addresses, phone numbers, and financial information, the primary legal bases are:

- **Performance of a Contract:** Processing is necessary for fulfilling a contract with the data subject or for pre-contractual steps requested by the data subject.
- **Compliance with Legal Obligations:** Processing is required to meet legal obligations to which BerryPax is subject.
- **Legitimate Interests:** Processing is necessary for the legitimate interests pursued by BerryPax or a third party, provided that such interests do not override the rights and freedoms of the data subject. Where none of these legal bases apply, BerryPax will obtain the data subject's explicit consent before processing their personal data.

For special categories of personal data (sensitive data), including health data and other sensitive information, processing will only occur under one of the following legal bases:

- **Explicit Consent:** The data subject has provided explicit consent for specific processing purposes.
- **Compliance with Legal Obligations or Rights:** Processing is necessary for legal compliance or the exercise of specific rights in employment, social security, or social protection law.
- **Legal Claims:** Processing is necessary for the establishment, exercise, or defense of legal claims.

2.2 Performance of a Contract

2.2.1 BerryPax collects and processes personal data when necessary for executing a contract to which the data subject is a party or for pre-contractual measures at the request of the data subject.

2.3 Compliance with Legal Obligations

2.3.1 BerryPax processes personal data to comply with legal obligations imposed by Union or Member State law.

2.4 Legitimate Interests

2.4.1 Where processing is based on legitimate interests, BerryPax ensures that such interests do not infringe on the rights and freedoms of the data subjects.

2.5 Consent

2.5.1 When processing relies on consent, BerryPax ensures that consent is freely given, specific, informed, and unambiguous.

2.6 Obligations and Specific Rights

2.6.1 Processing may be necessary to comply with obligations or exercise specific rights in the context of employment or social security law.

2.7 Legal Claims

2.7.1 Processing personal data may be necessary to establish, exercise, or defend legal claims.

BerryPax ensures that all processing activities adhere to applicable data protection laws and ethical standards, safeguarding the rights and privacy of data subjects.

---

3. Processing and Transfer of Personal Data

3.1 Role of BerryPax as Data Controller

3.1.1 BerryPax primarily acts as the data controller, determining the purpose and methods of processing personal data, particularly regarding clients, business partners, and employees.

3.2 Engagement of Data Processors

3.2.1 BerryPax may engage third-party data processors to handle personal data on its behalf, such as HR system providers and IT service providers. All data processors must adhere to BerryPax's documented instructions and comply with stringent security measures equivalent to those maintained by BerryPax. If a processor does not meet BerryPax's security standards, an alternative processor will be selected.

3.3 Data Processing Agreements

3.3.1 Prior to transferring personal data to a processor, BerryPax evaluates whether the processor provides adequate safeguards in accordance with GDPR requirements. A legally binding data processing agreement is established to ensure BerryPax retains control over data processing activities, even when data is handled outside its direct jurisdiction. 3.3.2 If a data processor or sub-processor operates

outside the European Union (EU) or the European Economic Area (EEA), the conditions outlined in section 3.4.2 apply.

3.4 Disclosure of Personal Data to Independent Data Controllers

3.4.1 Before disclosing personal data to an independent data controller, BerryPax ensures compliance with GDPR principles and verifies that a valid legal basis exists for such disclosure. 3.4.2 If transferring personal data to a third party outside the EU/EEA in a jurisdiction that does not provide an adequate level of data protection, BerryPax ensures appropriate safeguards, such as the execution of EU Standard Contractual Clauses, before proceeding with the transfer.

---

4. Rights of Data Subjects

Subject to various terms, conditions, and exceptions, data subjects have the following rights:

4.1 Duty of Information When Obtaining Personal Data from the Data Subject

4.1.1 When BerryPax processes data, including collecting and registering personal data about data subjects, BerryPax is obligated to inform individuals about:

- The intended purposes and legal basis for processing personal data.
- The categories of personal data involved.
- Legitimate interests pursued by BerryPax, if processing is based on a balancing of interests.
- Recipients or categories of recipients of the personal data, if any.
- Intention to transfer personal data to a third country and the legal basis for such transfer, if applicable.
- Duration for which personal data will be stored, or the criteria used to determine that period.
- Rights to request access, rectification, erasure, or restriction of processing, and the right to data portability.
- Right to withdraw consent at any time, if processing is based on consent.
- Right to lodge a complaint with BerryPax or a supervisory authority.
- Whether providing personal data is a statutory or contractual requirement, and the consequences of not providing such data.
- Existence of automated decision-making, including profiling, and meaningful information about its logic and consequences.

4.1.2 BerryPax has prepared a privacy notice containing a detailed description of these information obligations.

4.1.3 If personal data are not obtained from the data subject, they must also be informed about the data's source, including whether it is from publicly accessible sources.

4.2 Right to Access

4.2.1 Data subjects have the right to confirm whether BerryPax is processing their personal data. If processing is confirmed, they have the right to access their personal data and the information outlined in 4.1.1.

4.3 Right to Rectification

4.3.1 Data subjects have the right to request correction of inaccurate personal data without undue delay.

4.4 Right to Erasure (Right to Be Forgotten)

4.4.1 Data subjects have the right to request erasure of personal data, which BerryPax must comply with unless retention is required by law.

4.5 Right to Restriction of Processing

4.5.1 Data subjects have the right to request restriction of processing under certain circumstances.

4.6 Right to Data Portability

4.6.1 Data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format to transfer it to another organisation.

4.7 Right to Object

4.7.1 Data subjects can object to processing of personal data based on specific grounds related to their situation, including profiling.

4.8 Request Handling

Requests to exercise these rights should be addressed promptly and within 30 days. They will be forwarded to BerryPax’s Service Center for processing by the Data Protection Officer.

5. Data Protection by Design and Data Protection by Default

5.1 Guiding Principles for Data Protection

BerryPax adopts the principles of **Data Protection by Design** and **Data Protection by Default** as foundational elements in the development of new products, services, and technical solutions. These principles ensure that privacy and data protection are central to the organization's operations and integrated into the core functionality of its services. The following key principles guide BerryPax's approach to data protection:

1. **Privacy by Default**: All personal data is automatically protected in BerryPax's systems and business practices, ensuring that privacy settings are applied by default. Privacy considerations are embedded into the design and operational processes from the outset, minimizing the risk of data breaches or misuse.

2. **Privacy Embedded into Design**: Privacy is a core element of business processes and software design. It is a critical part of the functionality of all products and services, ensuring that privacy considerations do not compromise the usability of systems and applications.

3. **End-to-End Security—Full Lifecycle Protection**: BerryPax ensures that personal data is protected continuously throughout its lifecycle. From collection to processing, storage, and eventual deletion, appropriate measures, including encryption and authentication, are in place to safeguard the data at all stages.

4. **Client-Centric Privacy**: BerryPax acknowledges that clients own their personal data and have the right to control it. BerryPax's client-centric approach ensures that data protection measures respect the rights of clients, including their right to correction and erasure, in line with the principles of data minimization and transparency.

These principles are foundational to BerryPax's commitment to safeguarding the privacy of its clients and meeting regulatory compliance requirements while fostering trust through its business offerings.

5.1.1 Data Protection by Design

Data protection by design requires that privacy and data protection considerations be integral to the creation, development, and operation of new products, services, and processes. BerryPax integrates key data protection principles into the design phase of its offerings by:

1. **State-of-the-Art Technology**: BerryPax employs the latest technological advancements to ensure that data protection measures are up-to-date and capable of effectively securing personal data.

2. **Cost of Implementation**: When implementing data protection measures, BerryPax carefully evaluates the financial implications to ensure that privacy measures are both effective and sustainable.

3. **Nature, Scope, Context, and Purposes of Processing**: BerryPax thoroughly analyzes the specific nature, scope, context, and purpose of the data processing activities. This allows the company to tailor its data protection strategies to the requirements of each project.

4. **Risks to Rights and Freedoms**: BerryPax assesses the potential risks to the rights and freedoms of individuals resulting from the processing of personal data. This helps to identify any vulnerabilities and implement appropriate safeguards.

BerryPax applies these considerations alongside technical and organizational measures—such as pseudonymization, encryption, and access controls—to ensure that data protection principles, like data minimization and purpose limitation, are effectively incorporated into the design of new products and services.

5.1.2 Data Protection by Default

Data protection by default is concerned with minimizing the collection, processing, and retention of personal data to only what is necessary for the specific purpose for which it is being processed. BerryPax ensures that the following principles are adhered to:

1. **Implementation of Appropriate Measures**: BerryPax guarantees that only the minimum amount of personal data necessary for each specific processing purpose is collected, processed, and stored.

2. **Data Minimization**: By applying strict data minimization principles, BerryPax limits the amount of personal data collected, reducing the risk of over-collection and ensuring compliance with regulatory requirements.

3. **Careful Accessibility**: Personal data is not made accessible by default. Access is granted only when necessary, and data access controls are implemented to ensure that personal data is not exposed unnecessarily.

These measures are embedded into system designs, ensuring that data protection principles are automatically implemented and enforced through default settings, aligning with privacy regulations and safeguarding individuals' rights.

---

6. Records of Processing Activities

As a data controller, BerryPax is obligated to maintain detailed and accurate records of all processing activities that it conducts. These records are essential for ensuring transparency and accountability in data processing operations. The following key information must be included in the records:

1. **Name and Contact Details**: The identity of the data controller, including relevant contact details, is documented to provide clarity on who is responsible for data processing.

2. **Purposes of Processing**: BerryPax clearly defines and articulates the purposes for which personal data is processed, ensuring that data is only used for the purposes specified and lawful.

3. **Categories of Data and Data Subjects**: Detailed descriptions of the types of personal data being processed and the categories of data subjects involved (e.g., employees, clients, suppliers) are maintained.

4. **Recipients of Personal Data**: Information regarding individuals, organizations, or entities to whom personal data is disclosed, including third countries or international organizations, is thoroughly documented.

5. **Transfers to Third Countries**: If data is transferred outside the European Union (EU) or European Economic Area (EEA), BerryPax records the destination country and any safeguards implemented to ensure compliance with international data protection standards.

6. **Envisaged Time Limits for Data Erasure**: The company maintains records of the expected retention periods for each category of data and the criteria used to determine the duration of data storage.

7. **Security Measures**: A description of the technical and organizational security measures in place to protect personal data is included, highlighting the company's commitment to maintaining high standards of data protection.

BerryPax is committed to making these records available to relevant regulatory authorities upon request to demonstrate its compliance with data protection regulations.

---

7. Deletion of Personal Data

BerryPax follows the principle of **data retention minimization** and ensures that personal data is deleted when it is no longer necessary for the original purpose of processing or when retention is no longer required by law. Key principles guiding the deletion of personal data include:

1. **Legitimate Purpose**: Data will be deleted once there is no longer a legitimate business need for retaining the data or when the retention period has expired, as defined by relevant legal obligations.

2. **Retention Periods**: BerryPax has established retention periods for various categories of personal data, which are outlined in the **Data Retention and Information Sharing Policy**. This policy ensures that data is retained for no longer than necessary to comply with legal requirements or business needs.

---

8. Security of Processing (Risk Assessments)

8.1 Security Measures

BerryPax is committed to ensuring the security of personal data throughout the processing lifecycle by implementing appropriate technical and organizational measures, including:

1. **Pseudonymization and Encryption**: The company applies pseudonymization and encryption techniques to protect personal data from unauthorized access, ensuring confidentiality.

2. **Confidentiality, Integrity, Availability, and Resilience**: BerryPax ensures the confidentiality, integrity, availability, and resilience of its data processing systems to safeguard data against any form of breach.

3. **Data Restoration Capability**: In the event of an incident, BerryPax is capable of restoring data access and availability swiftly, minimizing disruption to business operations.

4. **Regular Testing and Evaluation**: Regular assessments and testing of security measures are conducted to evaluate their effectiveness and identify any potential vulnerabilities.

8.2 Risk Assessment

BerryPax conducts comprehensive risk assessments for each processing activity, taking into account factors such as the potential for accidental or unlawful destruction, loss, alteration, or unauthorized access to personal data. The company proactively addresses potential risks through strategic measures designed to mitigate them.

---

9. Data Protection Impact Assessment (DPIA)

A **Data Protection Impact Assessment (DPIA)** is conducted when processing activities are likely to result in high risks to the rights and freedoms of individuals. The DPIA includes:

1. **Risk Assessment**: BerryPax evaluates the nature, scope, context, and purposes of processing activities, identifying any potential risks to individuals' rights.

2. **Implementation of Safeguards**: Based on the DPIA, BerryPax implements appropriate measures to minimize identified risks and align processing with data protection requirements.

3. **Regular Reviews**: The technical and organizational measures identified in the DPIA are regularly reviewed and updated, with a minimum frequency of every six months, to ensure their ongoing relevance and effectiveness.

---

10. Profiling

10.1 Definition of Profiling

In accordance with the General Data Protection Regulation (GDPR), profiling refers to any form of automated processing of personal data that is used to evaluate certain personal aspects of a natural person. The aim of profiling is typically to analyze or predict aspects concerning the person's behavior, preferences, economic situation, health, reliability, or location.

10.2 Profiling at BerryPax

BerryPax uses profiling techniques to automate the analysis of personal data. This includes the evaluation of individual behaviors, preferences, or potential risks, but always within the bounds of privacy regulations. Any automated decisions resulting from profiling that significantly affect individuals will be handled with full compliance to GDPR guidelines, ensuring transparency, fairness, and accountability.

BerryPax engages in **profiling** for the following purposes:

1. **Identifying Financial Crime**: BerryPax uses profiling techniques to identify potential instances of financial crime, such as fraud or money laundering. By analyzing patterns in client behaviors and transactions, profiling helps detect anomalies that may indicate illicit activity, enabling proactive measures to prevent financial crime.

2. **Client and Lead Engagement**: Profiling is also utilized to enhance client and lead engagement by delivering personalized communications. This includes tailoring product and service recommendations to individuals based on their preferences, interests, and behaviors. Such profiling ensures that clients and leads receive the most relevant and valuable information, thereby enhancing user experience and engagement.

3. **Creditworthiness Assessment**: BerryPax uses profiling to assess an individual's creditworthiness. By analyzing historical data, behavioral trends, and other relevant information, the company is able to evaluate the financial stability of individuals and make informed decisions regarding lending or credit-related services.

BerryPax is committed to ensuring that all profiling activities are conducted in compliance with applicable data protection regulations, including the **General Data Protection Regulation (GDPR)**. The company prioritizes the rights and freedoms of individuals and implements appropriate safeguards to mitigate risks associated with profiling, ensuring transparency, fairness, and accountability in all profiling activities.

---

11. National Requirements

11.1 Compliance with GDPR

BerryPax is fully committed to adhering to the **General Data Protection Regulation (GDPR)** in all internal processes and procedures. This commitment ensures that personal data is handled in a lawful, fair, and transparent manner, with robust measures in place to safeguard the privacy and rights of individuals. BerryPax's

policies, procedures, and practices are structured to ensure compliance with the GDPR's requirements and to maintain the highest standards of data protection.

11.2 Adherence to Stricter National Legislation

In instances where national legislation imposes a higher level of protection for personal data than is mandated by the GDPR, BerryPax will adhere to these stricter legal requirements. This ensures that data processing activities meet or exceed the privacy standards set by national regulators.

Furthermore, if BerryPax's internal policies or guidelines set more stringent standards for data protection than local laws require, these internal policies will take precedence. Employees and stakeholders must comply with BerryPax's internal guidelines, particularly with regard to services provided or processing activities undertaken, to ensure uniformity and consistency in data protection practices across the organization.

This dual commitment—to both the **GDPR** and national legislation—demonstrates BerryPax's dedication to upholding the highest standards of data protection, while recognizing the need to respect and comply with diverse international and national regulatory frameworks.

---

12. Contact

For any inquiries related to the content of this data protection guideline, or to file a complaint regarding BerryPax's data processing activities, individuals are encouraged to contact **BerryPax's Privacy Team**. We take all concerns seriously and will address them promptly and professionally.

You may contact us at:
Email: privacy@berrypax.com

BerryPax is committed to fostering transparency, accountability, and compliance with data protection laws, and we value the feedback and input of our clients, partners, and stakeholders in our continuous efforts to enhance our data protection practices.
