DATA PROTECTION POLICY

This Policy covers Company and Staff procedures required to comply with the applicable data protection laws including the GDPR from a day-to-day perspective.

Contents

Related Policies

This Policy is supplemented by the following additional documents:

- Bocoy Distributors Ltd_Waterfront- Employee Privacy Notice
- Bocoy Distributors Ltd_Waterfront– Job Applicant Privacy Notice

Purpose

To describe the processes and procedures Bocoy Distributors Ltd_Waterfront has in place to comply with European Data Protection Laws. References in this Policy to "Bocoy Distributors Ltd_Waterfront", "us" shall mean Bocoy Distributors Ltd_Waterfront Restaurant unless otherwise specified.

This Policy is based on the following principles: **Lawfulness, Fairness & Transparency, Purpose Limitation, Data Minimisation, Data Accuracy, Data Retention, Security, International Transfers, Individuals' Rights and Accountability.**

Scope

This document forms part of the overall Bocoy Distributors Ltd_Waterfront Compliance Manual. It covers all Personal Data processed by Bocoy Distributors Ltd_Waterfront electronically or in structured paper files, specifically in its capacity as Data Controller.

It applies to all Bocoy Distributors Ltd_Waterfront directors, officers, and employees (which, for these purposes, includes temporary employees, agency personnel and contractors) (collectively, "**Personnel**"). Personnel are required to read, understand, and adhere to this Policy as well as applicable laws.

All Bocoy Distributors Ltd_Waterfront managers, officers, and directors are responsible for enforcing this Policy and ensuring that employees, individuals, and entities for which they are responsible are aware of, understand, and adhere to, the requirements of this Policy. Any breaches of this Policy must be reported to the Operations Manager, **Robert Rae** (nominated Compliance Officer).

Wilful or negligent failure by Personnel to comply with European Data Protection Laws or this Policy is a disciplinary offence and may be considered gross misconduct in some cases and will be handled in accordance with [Franchisee]'s disciplinary procedures.

Failure to comply with this Policy may also mean that Personnel are directly liable for penalties under European Data Protection Laws. In particular, unauthorised use by an individual, for private purposes, of Personal Data obtained through work at Bocoy Distributors Ltd_Waterfront is a criminal offence in some countries.

This Policy does not substitute any applicable national data protection and privacy laws, regulations and Codes of Conduct in countries where Bocoy Distributors Ltd_Waterfront operates but has been compiled with the UK interpretation of the General Data Protection Regulation ("GDPR") in mind. Local laws must be followed at all times and will take precedence over this Policy where they provide for stricter standards on privacy and data protection. Any variations will be set out in an Appendix to this Policy. Supplemental guidance for specific teams may be issued from time to time.

Consult with **Robert Rae** or with the Legal Team for any advice, help or support on any matter covered by this Policy. Any exceptions to this Policy must be approved by **Robert Rae**. If you are unsure about whether an issue is worth rising, err on the side of caution, and speak to this person.

Responsibility for Data Protection within Bocoy Distributors Ltd_Waterfront

Bocoy Distributors Ltd_Waterfront has elected not to formally appoint a Data Protection Officer ("DPO") on the basis that Bocoy Distributors Ltd_Waterfront's activities do not meet the requirements of Article 37(1) of the GDPR, specifically taking into consideration the Article 29 Working Party Guidelines on Data Protection Officers. External legal counsel was sought in this respect. Bocoy Distributors Ltd_Waterfront will continue to monitor this requirement and will appoint a formal DPO if required.

General Data Protection duties are instead coordinated by **Robert Rae** (200 77242).

Key Definitions

Data Controller is the legal or natural person which (alone or jointly with others) determines the purposes and means of Processing of Personal Data. For the purposes of this Policy, [Franchisee] is considered to be a Data Controller.

Data Processor means any legal or natural person that Processes Data on behalf of the Data Controller, for example, [Franchisee]'s external IT provider.

European Data Protection Laws means the EU Data Protection Directive (95/46/EC) and any legislation and/or regulation implementing or made pursuant to it (including the Data Protection Act 1998) and any law or regulation which amends, replaces, supplements or consolidates any of the foregoing (including the General Data Protection Regulation 2016/679 ("**GDPR**") from time to time.

Personal Data means any information relating to an identified or identifiable living individual such as our customers, operating partners, employees or any other individuals. Examples of Personal Data are name, address, date of birth, personal financial and banking information. An identifiable person is one who can be identified directly or indirectly, in particular, reference to an identifier such as a name, identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal Data includes Pseudonymous Data but not information which is truly anonymous. It can include opinions about individuals as well as facts and will include CCTV footage or audio recording. **The fact that information is publicly available (e.g. on LinkedIn) does not stop data protection laws applying to it.**

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

Pseudonymous Data means Personal Data which has been processed in such a manner that the Personal Data can no longer be attributed to a specific individual without the use of additional information.

Processing has a broad meaning that covers virtually anything we do with Personal Data, including the collection, storage, use, disclosure and destruction of the Personal Data. Personnel will almost certainly process some Personal Information about individual customers as well as other Personnel and business contacts.

Special Categories of Data are Personal Data that receive special legal protection under applicable law. They include **racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying an individual, health, or sex life or sexual orientation**. The processing of criminal conviction and offence data ("**Criminal Offence Data**") is additionally prohibited or restricted by applicable laws. For example, medical and other health information held about Personnel will be a special category of data.

Data Protection Policy Statement

The privacy of Bocoy Distributors Ltd_Waterfront's Personnel, vendors, operating partners, customers and other individuals about whom it processes Personal Data in the course of providing its investment management services is extremely important to Bocoy Distributors Ltd_Waterfront. Protecting their Personal Data and using it in a fair and trustworthy manner is key to Bocoy Distributors Ltd_Waterfront's core values and is an important part of maintaining its relationship and reputation with the its customers.

European Data Protection Principles

[Franchisee] is fully committed to complying with its obligations under European Data Protection Laws, whenever it is Processing Personal Data. To this end, Bocoy Distributors Ltd_Waterfront fully endorses the data protection principles set out below.

Principle 1: Lawfulness

We can only Process Personal Data where we have a lawful basis as set out in European Data Protection Laws. A lawful basis includes where we are Processing Personal Data:

- for our (or a third party's) legitimate business interests, provided these interests are not overridden by the rights or interests of the relevant individual (e.g. to ensure the effective management of our Personnel, or to ensure that our Personnel are delivering good customer service); or
- to comply with a legal obligation (e.g. for tax purposes, or to report an incident to law enforcement authorities).

The Processing of Personal Data can also be carried out with the consent of the relevant data subject, but as the requirements for obtaining valid consent under European Data Protection Laws will be particularly difficult for Bocoy Distributors Ltd_Waterfront to satisfy, Bocoy Distributors Ltd_Waterfront should avoid relying on this ground where possible. Consent may, however, still be required for marketing purposes and for use of cookies and similar technologies on Bocoy Distributors Ltd_Waterfront's websites.

Additional (and more restrictive) grounds apply to the Processing of Special Categories of Personal Data and Criminal Offence Data. These are very limited under European Data Protection Laws and in the context of investment data, only four grounds are of potential relevance. These include processing which is (i) in the substantial public interest, on the basis of Union or Member State law; (ii) data which has been manifestly made public by the data subject; (iii) criminal offence data which is permitted to be processed by Union or Member State law (which for UK purposes, we should anticipate that this can be processed on the same grounds as Special Categories of Data); or (iv) data which is processed with the explicit consent of the data subject.

- ➢ Personnel should ensure there is a lawful basis for any Processing of Personal Data for which they are responsible. Staff should seek guidance from **Robert Rae** if they wish to Process Personal Data based on consent.
- ➢ If Personal need to ask for additional Personal Data or are changing how Personal Data are processed, always consider if this Personal Data or the changes are for a lawful reason.

Principle 2: Fairness and transparency

In order to be fair and transparent, we must tell individuals how their Personal Data is Processed by us in a concise, transparent, intelligible and easily accessible way, using clear and plain language. This should include what Personal Data is collected, how we intend to use it, who we share it with, if we intend to transfer it to another country outside of the European Economic Area as well as how individuals can contact us with questions or in order to exercise their rights. For more detail on exactly what information needs to be provided to individuals, please see our Guidance Note on Fair and Lawful Processing of Investment Data.

We do this for our employees in our Employee Privacy Notice and for website visitors in our Bocoy Distributors Ltd_Waterfront Privacy & Cookies Policy.

- ➢ If Personnel need to ask for more Personal Data or change how Personal Data is Processed, always consider if further information needs to be given to relevant individuals. Personnel should pay particular attention to providing information on any uses of Personal Data which the individual would not expect.

Principle 3: Purpose Limitation

Personal Data must only be used for the purposes for which it was collected. Personnel should not use Personal Data for any purposes which we have not told the individual about or which would not be obvious to that individual (or compatible with the original purpose). For example:

- Personnel should only disclose Personal Data with others within their function or business where that person needs to know the information in order to perform their function in line with the specified purposes;
- In determining whether a new purpose of Processing is compatible with the original purpose, Personnel will need to consider any link between the Purposes, the context in which the Personal Data have been collected and the relationship between the parties, the nature of the Personal Data, the possible consequences of the future Processing and any proposed safeguards; and
- Use of Personal Data for new purposes may in some limited circumstances require notifications or authorisations to be made with relevant data protection authorities. It may also require consultation with workers' representatives. Personnel must consult with the **Robert Rae** if they have any queries about whether a particular use of Personal Data is permitted or wish to use Personal Data for a new purpose.

Principle 4: Data Minimisation

The Personal Data which we collect must be adequate, relevant and limited to that which is necessary for the purposes for which it is collected. We should not ask for more Personal Data than we need for the lawful basis for which we are collecting it. We shall make regular checks on the relevance of Personal Data being collected by Personnel to ensure it continues to be proportionate to the purpose.

The following data minimisation techniques should be considered wherever feasible:

- **Less is more**: Always ask yourself, do we need to collect this information to achieve our objectives? An example of over data collection would include sending a general questionnaire to job applicants, which includes specific questions about family members and relatives for which no use of the collected information will be made.
- **Anonymisation**: If a data set including Personal Data can be anonymized, then it should be. This reduces the risk of harm to the individuals concerned and removes such data from the scope of this policy (remember that data can only be considered to be genuinely anonymised if it is not possible to re-identify an individual from that data or other data in our possession).
- **Pseudonymisation:** If anonymisation is not possible, consider whether Personal Data can be subject to pseudonymisation, which is the technique of processing personal information such that it can no longer be attributed to a specific individual without the use of additional

information, which must be kept separately and be subject to technical and organisational measures to ensure non-attribution.

Principle 5: Data Accuracy

Personal Data must be accurate and up to date. We will encourage individuals to inform us of any changes to their Personal Data (and update, rectify or erase records as a result).

- Personnel should not use Personal Data they suspect might be out of date without confirming its accuracy.
- Personnel shall ensure that Personal Information is accurately captured and is managed in accordance with the business rules that apply to each system. Irrelevant or out of date information should be removed and securely deleted in accordance with our Data Retention Policy.
- Regular opportunities shall be given to Personnel to verify any Personal Data relating to them which is held by us and they should promptly notify the **Restaurant General Manager** of any changes in their Personal Data or circumstances which may affect the records held about them (e.g. address, bank details). Any changes shall be actioned promptly. In some cases, it may be necessary to request evidence to support a change. This is in line with the Business Continuity & Disaster Recovery Plan.
- If Personnel are told about a change in a customer or other individual's details, the relevant databases should be updated without delay.

Principle 6: Data Retention

Personal Data shall not be kept for longer than is required in order to meet the lawful purpose for which it was collected. It should then be securely deleted. This requirement is subject to other laws and obligations that require us to retain information for certain periods. For more details, see our **Employee Privacy Notice** (our data retention policy).

If Personal Data cannot be deleted (or anonymised) because for instance archived tapes are kept in a third party storage location, the above principle will be satisfied if such information has been 'put beyond use' provided that we:

- are not able, or will not attempt, to use the Personal Data to inform any decision in respect of any individual or in a manner that affects the individual in any way;
- do not give any other organisation access to the Personal Data;
- surround the Personal Data with appropriate technical and organisational security; and
- commit to permanent and secure deletion of the information if, or when, this becomes possible.

Principle 7: Security

Personal Data needs to be kept and used securely. It needs to be protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. This applies to our information systems, sites and our day to day handling of Personal Data. At a minimum, we will comply with any security and organizational measures required by law.

Further guidance is contained in the Acceptable Use Policy and the Information Security Policy, but in summary, some of the areas covered by these Security Standards and Policies include:

- Physical Security
- Data Discovery, Cataloguing and Classification
- Data Loss Prevention
- Data and Email Encryption
- Data Breach Identification and Blocking
- Data Portability
- Endpoint Security and Mobile Device Management ("MDM")
- Cloud Storage and Sharing Services
- Anti-Malware

- Identity and Access Management

Further detail of how Bocoy Distributors Ltd_Waterfront has implemented these measures is included in the Appendix.

Appointment of Data Processors

If Bocoy Distributors Ltd_Waterfront (as data controller) engages another organization to process Personal Data on its behalf, that organisation (the "Data Processor") must have implemented "appropriate technical and organizational measures" to meet the requirements of applicable European Data Protection Law and ensure the protection of individuals' rights. As part of this process, a written contract must be put in place with the Data Processor which contains specific contractual obligations.

Where Bocoy Distributors Ltd_Waterfront is acting as a Data Processor on behalf of the Master Franchisor (the Data Controller), it **cannot engage another processor without prior specific or general written authorisation of the Data Controller**. In the case of general written authorisation, Bocoy Distributors Ltd_Waterfront will need to inform the Data Controller of any intended changes concerning the addition or replacement of other processors, thereby giving the Data Controller the opportunity to object to such changes. It will also need to ensure that it flows down the relevant obligations to the sub-processors.

- Any member of staff responsible for appointing a Data Processor should ensure their contracts contain the appropriate provisions and that they have carried out a check of the Data Processor's security measures to ensure that they comply with Bocoy Distributors Ltd_Waterfront's requirements.
- Bocoy Distributors Ltd_Waterfront will carry out regular inspections and audits of its Data Processor's (and any sub-processors) systems, records, premises, personnel and any other materials used in the provision of the relevant services in order to check that the Data Processors is meeting its contractual obligations and any applicable obligations under European Data Protection Laws. An audit provision will be included in the written contracts.

Principle 8: International Transfers

European data protection rules restrict transfers of Personal Data outside the EEA (including to other group companies and external Data Processors) unless there is adequate protection for the Personal Data or prescribed steps have been taken to ensure the Personal Data is protected. Bocoy Distributors Ltd_Waterfront may on occasion exports to other parties located outside of the EEA. If we do so, we will do so pursuant to European Commission approved standard contractual clauses to regulate the transfers of certain Personal Data between us and other members of our Group.

All files containing personal information that are exported are subject to the same requirements outlined in the Information Security Standard. These describe the processes that should be followed by Personnel when exporting this data as well as the technological controls used to ensure onward processing is controlled.

There are a (limited) number of other circumstances where Personal Data can be transferred outside of the EEA, including:

- where it is being sent to a country or territory or international organisations recognized by the Commission as offering adequate protection (this would include to US organisations which are EU-US Privacy Shield Certified.);
- reliance on binding corporate rules;
- where the individual has explicitly consented to the transfer;
- where necessary to perform a contract;
- where necessary for reasons of important public interest; or
- where necessary for the establishment, exercise or defence of legal claims.

Seek advice from **Robert Rae** if:

- a third party will process Bocoy Distributors Ltd_Waterfront's Personal Data outside of the EEA (not only where the third party is based outside the EEA but also if the Personal Data will be held or remotely accessed by a third party or its subcontractors in a location outside of the EEA); or
- there are questions about what Personal Data may be transferred outside the EEA.

Principle 9: Individuals' Rights

We will always honour individuals rights under European Data Protection laws (to the extent applicable):

- to be given information about how their Personal Data is Processed (see Section on Fairness and Transparency above for more details);
- to access and rectify Personal Data relating to them;
- to erase or restrict Processing;
- to transfer Personal Data to another Data Controller;
- to object to direct marketing (including profiling linked to direct marketing) to them;
- to object to certain other types of processing in special situations; and
- to not be subject to the use of entirely automated decisions (including profiling) which produce legal effects or significantly affect the individuals.

We will respond to any requests without undue delay, and usually within one month of receipt of the request.

- Requests by Personnel to see their records or to exercise any of their other rights under data protection laws should made, in writing, to **Robert Rae** who will take appropriate steps to deal with the request made.
- Staff must take care when recording details in documents as those to whom the text refers (such as individual customers) may see this information at a later date. Information should only be entered which is appropriate, proportionate and justifiable.
- Requests to opt-out of marketing should be forwarded to **Robert Rae**.
- If Personnel receive any requests to see Personal Data from any other individuals (e.g. customers) or any other requests or complaints relating to the way in which their Personal Data is Processed by Bocoy Distributors Ltd_Waterfront, these should be immediately forwarded to the Head of Legal who will coordinate accordingly, referring to the Head of Operations, Robert Rae and Bocoy Distributors Ltd_Waterfront's external IT service provider where appropriate. There are often strict timescales for complying with such requests, so requests must be forwarded as soon as possible following receipt.

Principle 10: Accountability

European data protection laws require us to implement a wide range of measures to reduce our risk of breaching GDPR and to demonstrate that we are taking data governance seriously. A description of some of the measures we have put in place to meet these requirements are set out below.

Records of Processing Activity

Prior to GDPR, many data protection authorities (including the Information Commissioner's Office in the UK) required Data Controllers to notify the relevant Data Protection Authority about their Processing activities. These obligations are likely to disappear under GDPR. However, we will be obliged to maintain a record of processing activities in relation to the Personal Data which we process. This record is to be made available to a competent supervisory authority on request. Accordingly, relevant Personnel and their team must ensure they notify **Robert Rae** who will update Bocoy Distributors Ltd_Waterfront's record of processing.

Training and Guidance

Upon joining Bocoy Distributors Ltd_Waterfront, all Personnel are required to read this policy, agree to abide by its terms and provide an annual declaration to this effect. All Personnel who process Personal Data as a significant part of their function will receive appropriate training on data protection and security as part of their induction programme and there will be ongoing training for existing Personnel.

New Systems and Processes

European data protection laws require us to implement technical and organizational measures to show that we have considered and integrated data compliance measures into our Processing activities (known as “Data Protection by Design and by Default” principle).

We commit to this Principle by:

- Identifying privacy risks at the outset of any project or before the implementation of a new product, system or service and plan for them accordingly;
- Respecting the Data Minimization principle, ensuring Personal Data is pseudonymised where possible;
- Embedding privacy into our technologies, operations and information architectures and consult all relevant stakeholders;
- Maintaining the integrity and high standards of our products and services; and
- Striving to be transparent with individuals about what is done to protect their Personal Data.

Impact Assessments

Each new product, system or service developed or purchased by us which involves the Processing of any Personal Data: (i) that is not of a type currently being Processed or (ii) in a way that it is not currently being used for; or (iii) that might be perceived by our customers, employees or other relevant individuals, as being privacy intrusive will go through a privacy impact process to determine whether it implicates the rights and freedoms of the relevant individuals and whether or not the processing is considered to be “high risk”.

Where "high risk" processing is identified, a more thorough assessment (a "Data Protection Impact Assessment") will be required before it is commenced in accordance with GDPR.

A Data Protection Impact Assessment will include a description of the processing activities, the risks arising and measures adopted to mitigate those risks and in particular safeguards and security measures to protect Personal Data and comply with GDPR. In limited circumstances, we may be required to consult with the relevant individuals or the relevant data protection authority.

Audit

In order to demonstrate compliance with the Data Protection Principles and other applicable law requirements, we will undertake internal audits of our Processing activities from time to time. All Personnel must cooperate with these audits.

Appendix - Security Details

Physical Security

Physical security is of paramount importance to us and is crucial to ensure the safety and security of our equipment as well as the information that our Personnel use or manipulate. Physical Security measures are illustrated in the Information Security Policy.

- Desks should be kept clear of all documents containing Personal Data at the end of each day.
- Personal Data should be kept in a locked filing cabinet, drawer, or safe. If it is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.
- Dispose of waste paper securely.

Data Discovery, Cataloguing and Classifying

In addition to the above, we have implemented controls to ensure Personal Data is handled appropriately outside of our core systems. These include protecting and securing information such as:

- Copies of production databases containing personal data taken for testing, development, or analytics purposes;
- Spreadsheets and other data sources populated by exporting customer contact and profiling details for a mail merge (subject to the same standard of security as the core systems);
- Email archives which are likely to contain Personal Data that must be protected under European Data Protection Laws.

Controls that Personnel are expected to follow in this respect are documented in the Information Security Policy whereas detailed notes on how these resources are secured from a technical perspective are included in the Information Security Standard.

Data Loss Prevention

We control data loss through measures such as automatically blocking outgoing email, other messages and file movements that contain Personal Data that has not been protected by appropriate safeguards, e.g. data encryption.

In some situations encryption can be automatically applied to Personal Data when it is classified or identified in an email message or document attachment, while in other situations messages can be quarantined to enable an organizational response.

Data and Email Encryption

Encryption is one of the few specific technologies called out in the text of the GDPR, and its presence there essentially mandates its use by organizations. We have implemented measures to encrypt data while at rest and when be used or transmitted. This ensures that if a breach occurs on any system, the information remains confidential and does not trigger the GDPR penalties.

Data Breach Identification and Blocking

European Data Protection Laws require us to report Personal Data Breaches to the relevant data protection authority without undue delay (and where feasible within 72 hours) after becoming aware of the Personal Data Breach (unless this is unlikely to result in a risk to the rights and freedoms of the individual). We may also need to notify individuals in certain circumstances and we must document the Personal Data Breach in line with the Data Breach Policy.

We have therefore implemented measures to proactively sense that data has been breached, audit the extent of the breach, and create an appropriate organizational response.

- In the event any individual becomes aware of a Personal Data Breach, they must notify **Robert Rae** immediately and provide as much information as they have (including the nature and the consequences of the Personal Data Breach and any measures taken or proposed to mitigate any adverse effects). Examples of Personal Data Breaches include Personal Data being sent to an incorrect recipient, Personal Data being accessed without authority and paperwork or computers containing Personal Data being lost or stolen.

Data Portability

Further to section 5.9 on Individuals' Rights, data subjects have the right to request an export of their data in a usable format that can be given to another vendor or service provider to import into its service in certain circumstances. Whilst this specific requirement is of low likelihood and risk for the organisation, Bocoy Distributors Ltd_Waterfront uses widely available products (such as Office 365 and Microsoft Exchange for email) to facilitate this requirement.

Endpoint Security and Mobile Device Management ("MDM")

The GDPR requires computing devices to be protected from loss or theft through mobile device management capabilities, such as remote wipe and kill. A lost device could be the weak link in the data protection chain, leading to a data breach based on information stored on the device or accessible through still active user credentials. Bocoy Distributors Ltd_Waterfront has rolled out MDM to all its staff, with specific measures taken detailed in the Information Security Standard.

Cloud Storage and Sharing Services

Bocoy Distributors Ltd_Waterfront conducts a periodic review of documents shared externally to minimise the extent of sharing with external parties. Use of default restrictions (such as time-limited links) is also encouraged to restrict sharing by default without the need for user intervention. Measures taken by Bocoy Distributors Ltd_Waterfront to review these permissions are outlined in the Data Governance Model whereas measures embedded within the design of the system are described in the Information Security Standard.

- Any transfers of Personal Data must be done securely, whether externally or internally. When emailing or posting, double check that information is being sent to the right recipient.
- Be aware that those seeking information sometimes use deception. Before sending out any Personal Data to any third party, be sure of their identity. This may involve carrying out checks to verify their identity particularly if you are releasing information over the phone. If in doubt, contact Robert Rae.

Anti-Malware

While a successful malware infiltration can render computers unusable, of more serious concern under GDPR is the potential for malware to harvest credentials for user and administrator accounts. Harvested credentials can then be used to access data sources across the organization (both on-premises and in cloud services), including those containing personal and sensitive personal data.

Bocoy Distributors Ltd_Waterfront works closely with its managed IT service provider to ensure the strongest practical level of security is applied in this respect (predominantly through the use of anti-virus and intrusion detection software).

Identity and Access Management

A cohesive identity and access management system that seamlessly unifies employee identity across applications is a foundational requirement for GDPR compliance. Bocoy Distributors Ltd_Waterfront uses the latest identity management protocols (Windows 10 Azure Active Directory) to manage this aspect of GDPR Compliance]. Furthermore, user identities are connected to third party software providers using Single-Sign-On where appropriate. This ensures access can be controlled centrally (and quickly) across a number of applications in a uniform way.
25th May 2018.