Data Protection Policy

Innpact (Mauritius) Ltd

23 February 2022

Foreword

Innpact (Mauritius) Ltd (the "**Company**") ensures a high level of data protection when it collects and processes data. This concerns information relating to its customers, business partners and employees. The Company being registered in Mauritius and determines the purposes and means of the processing of personal data and has decision making power with respect to the processing, it is considered as a controller under the Data Protection Act 2017 ("DP Act 2017"). It must therefore comply with the provisions of the DP Act 2017.

This Data Protection Policy ("Policy") sets out strict requirements for processing personal data pertaining to customers, business partners and employees. It meets the requirements of the DP Act 2017. The Policy sets data protection principles, including transparency and data security.

The Company's employees, including trainees and any other person who provide services on behalf of the Company must adhere to the Policy. As the Data Protection Officer, it is my duty to ensure that the rules and principles of data protection at the Company are adhered to.

The Company may make amendments to this Policy, so please ensure that you view the latest version. An e-mail notifying you of the amendments will be sent by the Data Protection Officer.

If you do not feel confident in your knowledge or understanding of this Policy, or you have concerns regarding the implementation of this Policy, or have any queries on the Policy do not hesitate to contact me as soon as possible to seek advice.

A khoodaruth

Mrs. Bibi Aneza Khoodaruth

Data Protection Officer for Innpact (Mauritius) Ltd

First issued on 23 February 2022

I. DEFINITIONS 4

II. AIM OF DATA PROTECTION POLICY 5

III. SCOPE OF THE DATA PROTECTION POLICY 5

IV. PRINCIPLES FOR PROCESSING PERSONAL DATA 5

1. LAWFULNESS AND FAIRNESS 5
2. RESTRICTION TO A SPECIFIC PURPOSE 6
3. TRANSPARENCY 6
4. PURPOSE LIMITATION 6
5. STORAGE LIMITATION 6
6. ACCURACY OF DATA 7
7. CONFIDENTIALITY AND DATA SECURITY 7

V. RELIABILITY OF DATA PROCESSING 7

VI. CUSTOMER AND PARTNER DATA 7

1.1 DATA PROCESSING FOR A CONTRACTUAL RELATIONSHIP 7
1.2 DATA PROCESSING FOR ADVERTISING PURPOSES 7
1.3 CONSENT TO DATA PROCESSING 8
1.4 DATA PROCESSING PURSUANT TO LEGAL AUTHORIZATION 8
1.5 DATA PROCESSING PURSUANT TO LEGITIMATE INTEREST 8
1.6 PROCESSING OF SENSITIVE DATA 8
1.7 AUTOMATED INDIVIDUAL DECISIONS 8
1.8 USER DATA AND INTERNET 8

VII. EMPLOYEE DATA 9

1.1 DATA PROCESSING FOR THE EMPLOYMENT RELATIONSHIP 9
1.2 DATA PROCESSING PURSUANT TO LEGAL AUTHORISATION 9
1.3 COLLECTIVE AGREEMENTS ON DATA PROCESSING 9
1.4 CONSENT TO DATA PROCESSING 9
1.5 DATA PROCESSING PURSUANT TO LEGITIMATE INTEREST 9
1.6 PROCESSING OF SENSITIVE DATA 10
1.7 AUTOMATED DECISIONS 10
1.8 TELECOMMUNICATIONS AND INTERNET 10

VIII. TRANSMISSION OF PERSONAL DATA 11

IX. CONTRACT DATA PROCESSING 11

X. RIGHTS OF THE DATA SUBJECT 12

XI. CONFIDENTIALITY OF PROCESSING 12

XII. SECURITY OF PROCESSING 13

XIII. DATA PROTECTION CONTROL 13

XIV. DATA PROTECTION BREACHES 13

XV. RESPONSIBILITIES AND SANCTIONS 13

XVI. DATA PROTECTION OFFICER 14

I. Definitions

Anonymised data:	Data that does not itself identify any individual and that is unlikely to allow any individual to be identified through its combination with other data
Company:	Innpact (Mauritius) Ltd
Collect:	Does not include unsolicited information.
Consent:	Any freely given specific, informed and unambiguous indication of the wishes of a data subject, either by a statement or a clear affirmative action, by which he signifies his agreement to personal data relating to him being processed .
Controller:	A person who or public body which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to the processing.
Data subject:	An identified or identifiable individual, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.
Personal data breach:	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Processing:	An operation or set of operations performed on personal data or sets of personal data, whether or not by automated means such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Special categories of personal data	In relation to an individual, means personal data pertaining to, for example, their racial or ethnic origin, membership of a trade union, the commission or alleged commission of an offence by them or a criminal sentence.

II. Aim of Data Protection Policy

The Company is committed to ensure compliance with the DPA. This Policy is based on the DPA and sets out the framework conditions for the collection, processing and disclosing of personal data.

III. Scope of the Data Protection Policy

This Policy applies to the Company and extends to all processing of personal data which it collects or processes or any other person who carries out work on behalf of the Company involving the handling of personal data. Anonymised data, e.g. For statistical purposes is not subject to this Policy. This Data Protection Policy may be amended from time to time.

You have a crucial role to play in ensuring that the Company maintains the trust and confidence of the individuals about whom the Company processes personal data (including its own employees), complies with the Company's obligations and protecting the Company's reputation. This Policy therefore sets out what the Company expects from you in this regard.

The latest version of the Policy can be obtained from the Data Protection Officer or can be accessed on the Company internal platform.

IV. Principles for processing personal data

1. Lawfulness and fairness

In order to collect and process personal data for any specific purpose, the Company must always have a lawful basis for doing so. Without a lawful basis for processing, such processing will be unlawful and unfair and may have an adverse impact on the affected data subjects.

Processing of personal data will only be lawful where at least one of the lawful bases applies:

1. The data subjects have given their consent for one or more specific purposes.
2. The processing is necessary for the performance of a contract to which the data subject is a party (e.g., a contract of employment with the Company).
3. To comply with the Company's legal obligations (e.g., to deduct PAYE for its employees, where applicable).
4. To protect the vital interests of the data subject or another person (this will equate to a situation where the processing is necessary to protect the data subject's life).
5. To pursue the legitimate interests of the Company whose interests are not outweighed by the interests and rights of the data subjects.

It is important to note that there is no hierarchy between the lawful bases for processing, of which the data subject's consent is one. For a data subject's consent to be valid and provide a lawful basis, it must be:

1. Specific (not given in respect of multiple unrelated purposes)
2. Informed (explained in clear language)
3. Unambiguous and given by a clear affirmative action (silence or pre-ticked boxes will not be sufficient)
4. Freely and genuinely given

A data subject must be able to withdraw their consent as easily as they gave it.

Unless the Company is able to rely on another lawful basis for processing, a higher standard of explicit consent (where there can be no doubt that consent has been obtained, e.g., a signed document) will usually be required to process special categories of personal data, for automated decision-making and for transferring personal data outside Mauritius.

2. Restriction to a specific purpose

Personal data can be processed only for the purpose that was defined before the data was collected.

3. Transparency

The data subject must be informed of how their data are being handled. In that regard, any information which is provided by the Company to the data subject must be concise, easy to understand and written in plain language. If the Company has not been transparent about how it processes personal data, this will call the lawfulness and fairness of the processing in question.

In general, personal data must be collected directly from the data subject concerned. When the data is collected, the data subject must either be aware of, or informed of:

1. The identity of the controller
2. The purpose of data processing
3. Third parties or categories of third parties to whom the data might be transmitted

Where the Company obtains any personal data about a data subject from a third party (e.g., information on a shareholder information from the promoter of a fund), it must verify that it has collected the personal data in compliance with the DPA and on a lawful basis where the sharing of the personal data with the Company was clearly explained to the data subject.

4. Purpose limitation

Before processing personal data, you must determine whether and to what extent the processing of personal data is necessary to achieve the purpose for which it is undertaken.

Personal data may not be collected in advance and stored for potential future purposes unless required or permitted by law. The Company must only collect and process personal data for specified, explicit and legitimate purposes that have been communicated to the data subjects before the personal data have been collected.

The Company must ensure that it does not process any personal data obtained for one or more specific purposes for a new purpose that is not compatible with the original purpose. Where the Company intends to do so, it must inform the data subjects before using their personal data for the new purpose and, where the lawful basis relied upon for the original purpose was consent, obtain such consent again.

5. Storage limitation

Personal data that is no longer needed after the expiration of legal or business process-related periods must be deleted. There may be an indication of interests that merit protection or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally, or the corporate archive has evaluated the data to determine whether it must be retained for historical purposes.

6. Accuracy of data

Personal data on file must be correct, complete, kept up to date and must be corrected or deleted without delay when the Company discovers, or is notified, that the data are inaccurate.

7. Confidentiality and data security

Personal data that are collected and processed must be secured by appropriate technical and organisational measures against unauthorised access to, alteration of, disclosure of, accidental loss of and destruction of data in control of the Company.

The Company maintains appropriate technical and organisational measures for the processing of personal data considering the:

1. The nature, scope and purposes of the processing
2. The volume of the processing
3. The likelihood and severity of risks of the processing for the data subjects

The Company regularly evaluates and test the effectiveness of the technical and organisational measures. You are responsible for ensuring the security of the personal data you process in the performance of your duties. You must ensure that you follow all procedures that the Company has put in place to maintain the security of personal data.

You must not attempt to circumvent any administrative, physical or technical measures the Company has implemented as doing so may result in disciplinary action and in certain circumstances, may constitute a criminal offence under the laws of Mauritius.

V. Reliability of data processing

Collecting, processing and using personal data is permitted only under the following legal bases. One of these legal bases is also required if the purpose of collecting, processing and using the personal data is to be changed from the original purpose.

VI. Customer and partner data

1.1 Data processing for a contractual relationship

Personal data of the relevant prospects, customers and partners can be processed to establish, execute and terminate a contract. This also includes advisory services for the partner under the contract if this is related to the contractual purpose. Prior to a contract – during the contract initiation phase – personal data can be processed to prepare bids or purchase orders or to fulfil other requests of the prospect that relate to contract conclusion. Prospects can be contacted during the contract preparation process using the information that they have provided. Any restrictions requested by the prospects must be complied with. For advertising measures beyond that, you must observe the following requirements under V.1.2.

1.2 Data processing for advertising purposes

Customer loyalty or advertising measures are subject to further legal requirements. Personal data can be processed for advertising purposes or market and opinion research, provided that this is consistent with the purpose for which the data was originally collected. The data subject must be informed about the use of his/her data for advertising purposes. If data is collected only for advertising purposes, the disclosure from the data subject is voluntary. The data subject shall be informed that providing data for this purpose is voluntary. When communicating with the data subject, consent shall be obtained

from him/her to process the data for advertising purposes. When giving consent, the data subject should be given a choice among available forms of contact such as regular mail, e-mail and phone (Consent, see V.1.3).

If the data subject refuses the use of his/her data for advertising purposes, it can no longer be used for these purposes and must be blocked from use for these purposes. Any other restrictions from specific countries regarding the use of data for advertising purposes must be observed.

13 Consent to data processing

Data can be processed following consent by the data subject. Before giving consent, the data subject must be informed in accordance with IV.3. Of this Policy. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, such as telephone conversations, consent can be given verbally. The granting of consent must be documented.

14 Data processing pursuant to legal authorization

The processing of personal data is also permitted if national legislation requests, requires or allows this. The type and extent of data processing must be necessary for the legally authorised data processing activity and must comply with the relevant statutory provisions.

15 Data processing pursuant to legitimate interest

Legitimate interests are generally of a legal (e.g. Collection of outstanding receivables) or commercial nature (e.g. Avoiding breaches of contract). Personal data may not be processed for the purposes of a legitimate interest if, in individual cases, there is evidence that the interests of the data subject merit protection, and that this takes precedence. Before data is processed, it is necessary to determine whether there are interests that merit protection.

16 Processing of sensitive data

Sensitive personal data can be processed only if the law requires this or the data subject has given express consent. This data can also be processed if it is mandatory for asserting, exercising or defending legal claims regarding the data subject. If there are plans to process sensitive data, the Data Protection Officer must be informed in advance.

17 Automated individual decisions

Automated processing of personal data that is used to evaluate certain aspects cannot be the sole basis for decisions that have adverse legal consequences or could significantly impair the data subject. The data subject must be informed of the facts and results of automated individual decisions and the possibility to respond. To avoid erroneous decisions, a test and plausibility check must be made by an employee.

18 User data and internet

If personal data is collected, processed and used on websites or in apps, the data subjects must be informed of this in a privacy statement and, if applicable, information about cookies. The privacy statement and any cookie information must be integrated so that it is easy to identify, directly accessible and consistently available for the data subjects.

If use profiles (tracking) are created to evaluate the use of websites and apps, the data subjects must always be informed accordingly in the privacy statement. Personal tracking may only be done if it is permitted under national law or upon consent of the data subject. If tracking uses a pseudonym, the data subject should be given the chance to opt out in the privacy statement.

If websites or apps can access personal data in an area restricted to registered users, the identification and authentication of the data subject must offer sufficient protection during access.

VII. Employee data, applicable for companies with employees

11 Data processing for the employment relationship

In employment relationships, personal data can be processed if needed to initiate, carry out and terminate the employment agreement. When initiating an employment relationship, the applicants' personal data can be processed. If the candidate is rejected, his/her data must be deleted in observance of the required retention period, unless the applicant has agreed to remain on file for a future selection process. Consent is also needed to use the data for further application processes or before sharing the application with other companies in the group.

In the existing employment relationship, data processing must always relate to the purpose of the employment agreement if none of the following circumstances for authorized data processing apply.

If it should be necessary during the application procedure to collect information on an applicant from a third party, the requirements of the corresponding national laws have to be observed. In cases of doubt, consent must be obtained from the data subject.

There must be legal authorization to process personal data that is related to the employment relationship but was not originally part of performance of the employment agreement. This can include legal requirements, collective regulations with employee representatives, consent of the employee, or the legitimate interest of the company.

12 Data processing pursuant to legal authorisation

The processing of personal employee data is also permitted if national legislation requests, requires or authorizes this. The type and extent of data processing must be necessary for the legally authorised data processing activity and must comply with the relevant statutory provisions. If there is some legal flexibility, the interests of the employee that merit protection must be taken into consideration.

13 Collective agreements on data processing

If a data processing activity exceeds the purposes of fulfilling a contract, it may be permissible if authorized through a collective agreement. Collective agreements are agreements between employers and employee representatives, within the scope allowed under the relevant employment relations law. The agreements must cover the specific purpose of the intended data processing activity and must be drawn up within the parameters of national data protection legislation.

14 Consent to data processing

Employee data can be processed upon consent of the person concerned. Declarations of consent must be submitted voluntarily. Involuntary consent is void. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In certain circumstances, consent may be given verbally, in which case it must be properly documented.

15 Data processing pursuant to legitimate interest

Personal data can also be processed if it is necessary to enforce a legitimate interest of Innpact (Mauritius) Ltd. Legitimate interests are generally of a legal (e.g., filing, enforcing or defending against legal claims) or financial (e.g., valuation of companies) nature.

Personal data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the employee merit protection. Before data is processed, it must be determined whether there are interests that merit protection.

Control measures that require processing of employee data can be taken only if there is a legal obligation to do so or there is a legitimate reason. Even if there is a legitimate reason, the proportionality of the control measure must also be examined. The justified interests of the company in performing the control measure (e.g. Compliance with legal provisions and internal company rules) must be weighed against any interests meriting protection that the employee affected by the measure may have in its exclusion, and cannot be performed unless appropriate. The legitimate interest of the company and any interests of the employee meriting protection must be identified and documented before any measures are taken. Moreover, any additional requirements under national law (e.g. Rights of co-determination for the employee representatives and information rights of the data subjects) must be considered.

16 Processing of sensitive data

Sensitive personal data can be processed only under certain conditions. Sensitive data are data about racial and ethnic origin, political beliefs, religious or philosophical beliefs, union membership, and the health and sexual life of the data subject. Under national law, further data categories can be considered highly sensitive or the content of the data categories can be filled out differently. Moreover, data that relates to a crime can often be processed only under special requirements under national law.

The processing must be expressly permitted or prescribed under national law. Additionally, processing can be permitted if it is necessary for the responsible authority to fulfil its rights and duties in employment law. The employee can also expressly consent to processing.

If there are plans to process highly sensitive data, the Data Protection Officer must be informed in advance.

17 Automated decisions

If personal data is processed automatically as part of the employment relationship, and specific personal details are evaluated (e.g., as part of personnel selection or the evaluation of skills profiles), this automatic processing cannot be the sole basis for decisions that would have negative consequences or significant problems for the affected employee. To avoid erroneous decisions, the automated process must ensure that a natural person evaluates the content of the situation, and that this evaluation is the basis for the decision. The data subject must also be informed of the facts and results of automated individual decisions and the possibility to respond.

18 Telecommunications and internet

Telephone equipment, e-mail addresses, intranet and internet along with internal social networks are provided by the company primarily for work-related assignments. They are a tool and a company resource. They can be used within the applicable legal regulations and internal company policies. In the event of authorized use for private purposes, the laws on secrecy of telecommunications and the relevant national telecommunication laws must be observed if applicable.

There will be no general monitoring of telephone and e-mail communications or intranet/ internet use. To defend against attacks on the IT infrastructure or individual users, protective measures can be implemented for the connections to the Innpact (Mauritius) Ltd network that block technically harmful content or that analyse the attack patterns. For security reasons, the use of telephone equipment, e-mail addresses, the intranet/internet and internal social networks can be logged for a temporary period. Evaluations of this data from a specific person can be made only in a concrete and justified case of suspected violations of laws or policies of Innpact (Mauritius) Ltd. The evaluations can be conducted only by investigating departments while ensuring that the principle of proportionality is met.

VIII. Transmission of personal data

If data is transmitted to a recipient outside Mauritius, the recipient must agree to maintain a data protection level, at least, equivalent to this Policy. This does not apply if transmission is based on a legal obligation.

If data is transmitted by a third party to the Company, it must be ensured that the data can be used for the intended purpose.

If personal data is transferred from the Company to another company within the group with its registered office outside of Mauritius, (third country), the company importing the data is obligated to cooperate with any inquiries made by the relevant supervisory authority in the country in which the party exporting the data has its registered office, and to comply with any observations made by the supervisory authority with regard to the processing of the transmitted data. The same applies to data transmission by a company in the group from other countries.

If a data subject claims that this Policy has been contravened by the company in the group located in a third country that is importing the data, the company that is located in Mauritius and is exporting the data undertakes to support the party concerned, whose data was collected in Mauritius, in establishing the facts of the matter and also asserting his/her rights in accordance with this Policy against the company of the group importing the data. In addition, the data subject is also entitled to assert his or her rights against the company exporting the data. In the event of claims of a violation, the company exporting the data must document to the data subject that the company importing the data in a third country (in the event that the data is further processed after receipt) did not violate this Policy.

IX. Contract data processing

Data processing on behalf of the Company means that a provider is hired to process personal data of the Company, without the provider being assigned responsibility for the related business process. In these cases, an agreement on data processing on behalf of the Company must be concluded with external providers. The Company retains full responsibility for correct performance of data processing. The provider can process personal data only as per the instructions from the Company. When issuing the order, the following requirements must be complied with; the department placing the order must ensure that they are met.

1. The provider must be chosen based on its ability to cover the required technical and organisational protective measures.
2. The order must be placed in writing. The instructions on data processing and the responsibilities of the client and provider must be documented.
3. The contractual standards for data protection provided by the Data Protection Officer must be considered.
4. Before data processing begins, the client must be confident that the provider will comply with the duties. A provider can document its compliance with data security requirements by presenting suitable certification. Depending on the risk of data processing, the reviews must be repeated on a regular basis during the term of the contract.
5. In the event of cross-border contract data processing, the relevant national requirements for disclosing personal data abroad must be met. In particular, personal data from Mauritius can be processed in a third country only if the provider can prove that it has a data protection

standard equivalent to this Policy or with the provisions of the DP Act 2017. Suitable tools can be:

a) Agreement on contract clauses for contract data processing in third countries with the provider and any subcontractors.

b) Participation of the provider in a certification system accredited by the DPO for the provision of a sufficient data protection level.

X. Rights of the data subject

Every data subject has the following rights. Their assertion is to be handled immediately by the responsible unit and cannot pose any disadvantage to the data subject.

a) The data subject may request information on which personal data relating to him/her has been stored, how the data was collected, and for what purpose. If there are further rights to view the employer's documents (e.g. Personnel file),if applicable, for the employment relationship under the relevant employment laws, these will remain unaffected.

b) If personal data is transmitted to third parties, information must be given about the identity of the recipient or the categories of recipients.

c) If personal data is incorrect or incomplete, the data subject can demand that it be corrected or supplemented.

d) The data subject can object to the processing of his or her data for purposes of advertising or market/opinion research. The data must be blocked from these types of use.

e) The data subject may request his/her data to be deleted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed.

f) The data subject generally has a right to object to his/her data being processed, and this must be taken into account if the protection of his/her interests takes precedence over the interest of the data controller owing to a particular personal situation. This does not apply if a legal provision requires the data to be processed.

g) The data subject has the right to withdraw his/her consent at any time without having to explain why. The lawfulness of processing based on consent before the withdrawal is not affected.

XI. Confidentiality of processing

Personal data is subject to data secrecy. Any unauthorized collection, processing, or use of such data by employees,if applicable, is prohibited. Any data processing undertaken by an employee that he/she has not been authorized to carry out as part of his/her legitimate duties is unauthorized. The "need to know" principle applies. Employees,if applicable, may have access to personal information only as is appropriate for the type and scope of the task in question. This requires a careful breakdown and separation, as well as implementation, of roles and responsibilities.

Employees,if applicable, are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorized persons, or to make it available in any other way. Supervisors must inform their employees at the start of the employment relationship about the obligation to protect data secrecy. This obligation shall remain in force even after employment has ended.

XII. Security of processing

Personal data must be safeguarded from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification or destruction. This applies regardless of whether data is processed electronically or in paper form. Before the introduction of new methods of data processing, particularly new IT systems, technical and organizational measures to protect personal data must be defined and implemented. These measures must be based on the state of the art, the risks of processing, and the need to protect the data (determined by the process for information classification).

In particular, the responsible department can consult with IT Department. The technical and organizational measures for protecting personal data must be adjusted continuously to the technical developments and organisational changes.

XIII. Data protection control

Compliance with this Policy and the applicable data protection laws is checked regularly with data protection audits and other controls. The performance of these controls is the responsibility of the Data Protection Officer, and other company units with audit rights or external auditors hired. The results of the data protection controls must be reported to the Company's board of directors. The Company's board of directors must be informed of the primary results as part of the related reporting duties. On request, the results of data protection controls will be made available to the Data Protection Office. The Data Protection Office can perform its own controls of compliance with the regulations of this Policy, as permitted under the law.

XIV. Data protection breaches

All employees (including any other person handling personal data on behalf of the Company) ,if applicable, must inform their supervisor immediately about cases of violations against this Policy or other regulations on the protection of personal data (data protection incidents). The manager responsible for the function or the unit is required to inform the Data Protection Officer immediately about data protection breaches.

In cases of:

1. improper transmission of personal data to third parties,
2. improper access by third parties to personal data, or
3. loss of personal data

The required company reports must be made immediately so that any reporting duties under the law can be complied with.

XV. Responsibilities and sanctions

Companies forming part of a group are required to ensure that the legal requirements, and those contained in this Policy, for data protection are met (e.g., national reporting duties). Management staff,if applicable, are responsible for ensuring that organizational, HR, and technical measures are in place so that any data processing is carried out in accordance with data protection… Compliance with these requirements is the responsibility of the relevant employees, if applicable. If official agencies perform data protection controls, the Chief Officer Corporate Data Protection must be informed immediately.

The departments responsible for business processes and projects must inform the Data Protection Officer in good time about new processing of personal data. For data processing plans that may pose special risks to the individual rights of the data subjects, the Data Protection Officer must be informed before processing begins. This applies in particular to extremely sensitive personal data. The managers

must ensure that the employees,if applicable, under their supervision are sufficiently trained in data protection.

Improper processing of personal data, or other violations of the data protection laws, can be criminally prosecuted and result in claims for compensation of damage. Violations for which individual employees,if applicable, are responsible can lead to sanctions under employment law.

XVI. Data Protection Officer

The Data Protection Officer works towards the compliance with Data Protection Laws. [She]/He is responsible for this Policy and supervises its compliance.

Any data subject may approach the Data Protection Officer at any time to raise concerns, ask questions, request information or make complaints relating to data protection or data security issues. If requested, concerns and complaints will be handled confidentially.

Contact details for the Data Protection Officer are as follows:

Mrs. Bibi Aneza Khoodaruth

aneza.khoodaruth@innpact.com