Data Protection Compliance Manual

VLH Ltd

31 October 2018

Table of contents

1. Introduction

1.1. VLH Ltd (the "Enterprise") consists of several companies as defined in **Annex 1**.

1.2. In the course of its business activities, the Enterprise processes personal data.

1.3. The purpose of this Data Protection Compliance Manual (the "Manual") is to set out the measures which the Enterprise has put in place to ensure that such processing is carried out in accordance with all applicable data protection legislation.

2. Definitions

2.1. In this Manual, the following words and expressions shall have the following meanings:

2.1.1. "Act" mean the Data Protection Act 2017, as amended or replaced from time to time;

2.1.2. "Data subject" means 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;

2.1.3. "Personal data" means any information relating to a data subject;

2.1.4. "Processing" means 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; and

2.1.5. "Special categories of data" in relation to a data subject means personal data pertaining to –

(a) his racial or ethnic origin;
(b) his political opinion or adherence;
(c) his religious or philosophical beliefs;
(d) his membership of a trade union;
(e) his physical or mental health or condition;
(f) his sexual orientation, practices or preferences;
(g) his genetic data or biometric data uniquely identifying him;
(h) the commission or alleged commission of an offence by him;
(i) any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any Court in the proceedings; or
(j) such other personal data as the Data Protection Commissioner may determine to be sensitive personal data.

3. Registration under the Act

3.1. The Enterprise shall be registered with the Data Protection Office established under Section 4 of the Act.

3.2. The Enterprise shall ensure that:

3.2.1. such registration is renewed periodically, prior to its expiry; and

3.2.2. the Data Protection Office is informed of any relevant change in the particulars of the Enterprise,

in accordance with the Act.

4. Data Protection Officer

4.1. The Enterprise shall appoint an officer within the Enterprise who shall be responsible for data protection compliance issues (the "Data Protection Officer").

4.2. The Data Protection Officer shall be designated on the basis of professional qualities and, in particular, knowledge of data protection law and practices and knowledge of the operations of the Enterprise.

4.3. The duties of the Data Protection Officer shall be as follows:

4.3.1. to inform and advise the Enterprise and the employees who carry out processing of their obligations pursuant to applicable data protection laws and this Manual;

4.3.2. to monitor compliance with applicable data protection laws and this Manual;

4.3.3. to cooperate with the Data Protection Office; and

4.3.4. to act as the contact point for the Data Protection Office on issues relating to processing.

4.4. The Data Protection Officer shall, in the performance of his or her tasks,

4.4.1. be independent; and

4.4.2. have due regard to the risks associated with processing operations, taking into account the nature, scope, context and purposes of processing.

5. Data Protection Policy

5.1. Rogers and Company Ltd, the parent company of the Enterprise, has adopted the Data Protection Policy set out in **Annex 2** for the Rogers Group and the Enterprise shall abide by same.

6. Lawful processing

6.1. The Enterprise shall not process personal data unless:

6.1.1. the data subject consents to the processing for one or more specified purposes; or

6.1.2. the processing is necessary:

6.1.2.1. for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;

6.1.2.2. for compliance with any legal obligation to which the Enterprise is subject;

6.1.2.3. for the purpose of historical, statistical or scientific research; or

6.1.2.4. for such other lawful purpose as may be authorised by law.

7. Collection of personal data

7.1. The Enterprise shall not collect Personal data unless:

7.1.1. it is done for a lawful purpose connected with a function or activity of the Enterprise; and

7.1.2. the collection of the Personal data is necessary for that purpose.

7.2. The purposes for which the Enterprise shall collect Personal data shall be as follows:

7.2.1. to provide services to its clients;

7.2.2. to enter into contractual relationships with suppliers and service providers and execute such contracts;

7.2.3. to keep a database of clients and potential clients to communicate with in respect of its services and matters related thereto;

7.2.4. to comply with its legal obligations towards authorities, including the Mauritius Revenue Authority, the Registrar of Companies and the regulators;

7.2.5. to keep a database of candidates who have sent CVs to the Enterprise, for potential future use;

7.2.6. to keep appropriate employment-related information on employees;

7.2.7. to provide facilities and benefits to its employees;

7.2.8. for security purposes;

7.2.9. to generate statistics and reports on different aspects of its business; and

7.2.10. for such other purposes as may be related, directly or indirectly, to its business activities.

7.3. When collecting personal data directly from a data subject, the Enterprise shall, at the time of collecting the personal data, ensure that the data subject is informed of the following, unless the data subject is already in possession of such information:

7.3.1. the identity and contact details of the Enterprise and the Data Protection Officer;

7.3.2. the purpose for which the data is being collected;

7.3.3. the intended recipients of the data;

7.3.4. whether or not the supply of the data by that data subject is voluntary or mandatory;

7.3.5. the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

7.3.6. the existence of the right to request from the Enterprise access to and rectification, restriction or erasure of personal data concerning the data subject or to object to the processing;

7.3.7. the existence of automated decision making, including profiling, and information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;

7.3.8. the period for which the personal data shall be stored;

7.3.9. the right to lodge a complaint with the Data Protection Commissioner (as defined in the Act);

7.3.10. where applicable, that the Enterprise intends to transfer personal data to another country and on the level of suitable protection afforded by that country; and

7.3.11. any further information necessary to guarantee fair processing in respect of the data subject's personal data, having regard to the specific circumstances in which the data is collected.

7.4. In order to inform data subjects of the matters set out at paragraph 7.3 above, the Enterprise shall:

7.4.1. adopt the Data Protection Notice set out in **Annex 3** (the "Notice"), which provides for the said matters;

7.4.2. display the Notice on its website;

7.4.3. add a link to the Notice in all emails emanating from the Enterprise and/or its employees, encouraging the recipients of the said emails to consult the Notice;

7.4.4. use its best endeavours to add a clause in all agreements to which the Enterprise is a party (including employment contacts) referring to the Notice (with a link to where the Notice may be consulted) and providing that personal data is collected by the Enterprise in accordance with the said Notice; and

7.4.5. add a reference to the Notice (with a link to where the Notice may be consulted) on:

7.4.5.1. all documents used by the Enterprise to collect personal data, including contact forms, forms to be filled by employees, clients or suppliers, quotations sent to clients, and so on; and

7.4.5.2. social media platforms used by the Enterprise to collect personal information.

8. Personal data of children

8.1. The Enterprise shall not knowingly process the personal data of a child below the age of 16 years unless consent is given by the child's parent or guardian.

8.2. Where the personal data of a child below the age of 16 years is involved, the Enterprise shall make every reasonable effort to verify that consent has been given or authorised, taking into account available technology.

9. Personal data breach

9.1. A personal data breach is 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 by the Enterprise.

9.2. In the case of a personal data breach, the Enterprise shall forthwith inform the Data Protection Officer who shall, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Data Protection Commissioner by filling the notification of personal data breach form set out in **Annex 4** and sending same to the Data Protection Commissioner.

9.3. Where, in the opinion of the Data Protection Officer, the personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the Enterprise shall inform the data subject of the personal data breach and provide a copy of the notification of personal data breach form sent to the Data Protection Commissioner to the data subject.

9.4. The communication of a personal data breach to the data subject shall not be required where:

9.4.1. the Enterprise has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the breach, in particular, those that render the data unintelligible to any person who is not authorised to access it, such as encryption;

9.4.2. the Enterprise has taken subsequent measures to ensure that the high risk to the rights and freedoms of the data subject referred to above is no longer likely to materialise; or

9.4.3. it would involve disproportionate effort and the Enterprise has made a public communication or similar measure whereby data subject is informed in an equally effective manner.

10. Duty to destroy personal data

10.1. Where the purpose for keeping personal data has lapsed, the Enterprise shall destroy the data as soon as is reasonably practicable thereafter.

10.2. The purpose for keeping personal data shall not be deemed to have lapsed for as long as processing such personal data is necessary:

10.2.1. for the Enterprise to fulfil the purposes it collected it for;

10.2.2. for the performance of any contract which may exist between the Enterprise and the data subject;

10.2.3. for the Enterprise to share with the data subject the latest news regarding the Enterprise and its services;

10.2.4. for the Enterprise to keep a record of the preferences of the data subject in order to service him again on future occasions;

10.2.5. for the Enterprise to satisfy any legal requirement, including statutory reporting obligations;

10.2.6. for the keeping of adequate records for historical, financial or statistical purposes;

10.2.7. for security purposes;

10.2.8. for the prevention of fraud and abuse; and

10.2.9. for the Enterprise to defend or enforce its rights.

10.3. The legal prescription period in Mauritius (i.e. the period during which one party may sue another after the happening of an event) is 10 years for non-immovable-property-related matters. Depending on the nature of the Enterprise's relationship with the data subject, the Enterprise may, in this context, choose to keep personal data for at least the legal prescription period in order for it to defend or enforce its rights.

10.4. In some circumstances, the Enterprise may anonymise personal data by pseudonymisation or encryption, such that the personal data can no longer be associated with data subjects, for research or statistical purposes, in which case the Enterprise may use this information indefinitely without further notice to the data subject.

11. Security of processing

11.1. The Enterprise shall use its best endeavours to implement the security and organisational measures set out in **Annex 5** for the prevention of unauthorised access to, the alteration of, the disclosure of, the accidental loss of and the destruction of the data within its control.

11.2. In addition, the Enterprise shall abide by and implement the measures set out in any IT or Information Security Policy adopted by Rogers and Company Ltd for the Rogers Group from time to time.

12. Record of processing operations

12.1. The Enterprise is required, as per law, to keep a record of all processing operations under its responsibility.

12.2. The matters pertaining to which records must be kept are described in detail in the Notice (**Annex 3**) and at paragraph 11 of the Manual.

13. Data protection impact assessment

13.1. The Enterprise shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data where the following processing operations are carried out:

13.1.1. a systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the individual or significantly affect the individual;

13.1.2. processing on a large scale of special categories of data;

13.1.3. a systematic monitoring of a publicly accessible area on a large scale; or

13.1.4. any other processing operations for which consultation with the Data Protection Office is required.

13.2. The assessment shall be carried out as follows:

13.2.1. Management shall fill the Data Protection Impact Assessment Form set out in **Annex 6**;

13.2.2. Management shall then send the filled-in Data Protection Impact Assessment Form to the Data Protection Officer, who shall review same and add his comments therein. The Data Protection Officer may seek the assistance of Rogers Legal for same; and

13.2.3. the Data Protection Impact Assessment Form, with the comments of the Data Protection Officer, shall then be sent to the Head of Internal Audit & Risk Management of Rogers and Company Ltd for his review.

13.3. Where upon reviewing the Data Protection Impact Assessment Form the Head of Internal Audit & Risk Management is of the opinion that the envisaged processing operations are by virtue of their nature, scope or purposes, likely to present a high risk:

13.3.1. he shall inform Management of same; and

13.3.2. the Enterprise shall consult the Data Protection Office prior to processing personal data in order to mitigate the risks involved for the data subjects.

14. Transfer of personal data outside Mauritius

14.1. The Enterprise shall not transfer personal data outside Mauritius unless:

14.1.1. it has obtained the prior approval of the Data Protection Commissioner;

14.1.2. it has obtained the consent of the data subject; or

14.1.3. the transfer is necessary:

14.1.3.1. for the performance of a contract between the data subject and the Enterprise or the implementation of pre-contractual measures taken at the data subject's request;

14.1.3.2. for the conclusion or performance of a contract concluded in the interest of the data subject between the Enterprise and another person;

14.1.3.3. for the establishment, exercise or defence of a legal claim; or

14.1.3.4. for such other purpose as may be authorised by law.

15. Access to personal data

15.1. Where the Enterprise receives a reasonable written request from a data subject to confirm whether the Enterprise is processing his personal data and/or to forward a copy of the data to him, the Enterprise shall, through the Data Protection Officer, comply with the request, subject to the exceptions and provisos set out below, in the following manner:

15.1.1. within a period of 3 business days from the date on which it receives the request, the Enterprise shall inform the data subject that his request has been received and is being processed;

15.1.2. within a period of 10 business days from the date on which it receives the request, the Enterprise shall send to the data subject:

15.1.2.1. a copy of the Data Protection Notice; and

15.1.2.2. the information set out in **Annex 7** in respect of the personal data of the data subject.

15.2. Where the request is made verbally, the Enterprise shall request the data subject to confirm same in writing.

15.3. A request shall be considered reasonable where:

15.3.1. it is the first time such a request is being made by the data subject; or

15.3.2. at least 12 months have elapsed since the last similar request made by the data subject; or

15.3.3. since the last similar request made by the data subject, there has been a change in the personal data of the data subject being processed or the processing operations relating to same.

15.4. Where the Enterprise receives an unreasonable request, or where the Enterprise is unable to determine whether a request is reasonable, it shall forthwith refer the matter to Rogers Legal for advice on how to proceed.

15.5. Where the Enterprise has any doubt concerning the identity of a person making a request, it shall request the data subject to provide a copy of his national identity card or passport before processing the request. Where the Enterprise still cannot establish the identity of the person making the request, it shall refer the matter to Rogers Legal for advice on how to proceed.

16. Rectification of personal data

16.1. On being notified in writing of the inaccuracy or incompleteness of personal data by a data subject to whom such data pertains, the Enterprise shall notify the Data Protection Officer and cause the data to be rectified or completed within 10 business days. Where such notification is made verbally, the Enterprise shall request the data subject to confirm same in writing before proceeding further.

17. Erasure of personal data

17.1. The Enterprise shall notify the Data Protection Officer and cause personal data to be erased from its records where:

17.1.1. the data subject withdraws his consent or objects to the personal data being processed; and

17.1.2. there is no other legal ground or overriding legitimate grounds for processing the personal data.

17.2. Where the Enterprise has made the personal data public, he shall take all reasonable steps to inform third parties processing such data, that the data subject has requested the erasure of any links to, or copy or replication of, that personal data.

17.3. The Enterprise shall not be required to erase personal data where the processing of personal data is necessary:

17.3.1. for reasons of public interest in the field of public health;

17.3.2. for the purpose of historical, statistical or scientific research;

17.3.3. for compliance with a legal obligation to process the personal data to which the Enterprise is subject; or

17.3.4. for the establishment, exercise or defence of a legal claim.

17.4. The Enterprise shall inform the data subject in writing whether:

17.4.1. the personal data has been erased; or

17.4.2. the Enterprise has elected not to erase the personal data and the reasons for such decision.

17.5. Where the Data Protection Officer is unable to determine whether personal data should be erased upon a request being made by a data subject, he shall refer the matter to Rogers Legal.

18. Direct marketing

18.1. The Enterprise shall not process personal data for direct marketing if the data subject objects to same.

19. Data Protection Register

19.1. The Data Protection Officer shall keep a Data Protection Register, in a format similar to the format set out in **Annex 8**, where he shall record the following matters, including the manner in which such matters have been dealt with:

19.1.1. personal data breaches;
19.1.2. data protection impact assessments;
19.1.3. requests for access to personal data;
19.1.4. requests for rectification of personal data;
19.1.5. requests for erasure of personal data;
19.1.6. objections to processing for direct marketing purposes; and
19.1.7. such other relevant matters relating to the processing of personal data.

The Data Protection Register shall be tabled at a meeting of the board of directors of the Enterprise once every year, or at such other interval as may be determined by the board.

Annex 1

The List of entities that form part of the Enterprise

Entity	Business Activity
VLH Ltd	Tourism and hospitality
Veranda Tamarin Ltd	- Wholesale trade - Transport by road - General retailer - Owns hotels - Owns and manages fitness centres - Restaurants (including liquor & other alcoholic beverages) with entertainment - Retail sale of other goods in specialised stores
Heritage Golf Club Ltd	- Wholesale trade - Retail sale of other goods in specialised stores
VLH Training Ltd	- Training Institution / (Education)
Seven Colours Spa Lt	- Distributor of general merchandise - Tourism
Heritage Events Co Ltd	- Business/Professional and Management Consultancy Service (including medical and para-medical practitioners and optician)(Firm)

Annex 2

The Data Protection Policy

We, the data controllers and data processors of the Rogers Group**:**

Shall endeavour to:

- Ensure that we are duly registered as controllers and/or processors with the Data Protection Commissioner.
- Ensure that personal data is:
  - processed lawfully, fairly and in a transparent manner;
  - collected for explicit, specified and legitimate purposes;
  - adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
  - accurate and, where necessary, kept up to date;
  - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; and
  - processed in accordance with the rights of data subjects.
- Inform data subjects of all relevant matters relating to the collection of their personal data, including the purpose for which the data is being collected and the period for which the data will be stored.
- Adopt policies and implement appropriate technical and organisational measures so as to ensure that the processing of personal data is performed in accordance applicable data protection legislation.
- Maintain a record of all processing operations under our responsibility.
- On the written request of a data subject, provide confirmation to him as to whether or not personal data relating to him is being processed and forward to him a copy of the data.
- On being informed of the inaccuracy of personal data by a data subject to whom such data pertains, cause the data to be rectified without undue delay.
- Destroy, as soon as reasonably practicable, personal data where the purpose for which the data was collected has lapsed.
- Notify the Data Protection Commissioner and the relevant data subjects, where applicable, of any personal data breach in a timely manner.

Where processing operations are likely to result in a high risk to the rights and freedoms of data subjects, carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data.

Shall endeavour not to:

- Collect personal data unless: (a) it is done for a lawful purpose connected with one of our functions or activities; and (b) the collection of the data is necessary for that purpose.

- Process personal data unless:
  - the data subject consents to the processing; or
  - the processing is necessary:
    - for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
    - for compliance with any legal obligation to which we are subject;
    - for the legitimate interests pursued by us, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or
    - for such other purpose as may be authorised by law.
- Process the personal data of a data subject who has objected in writing to such processing unless we demonstrate compelling legitimate grounds for the processing which override the data subject's interests, rights and freedoms or for the establishment, exercise or defence of a legal claim.
- Process the personal data of a child below the age of 16 years unless consent is given by the child's parent or guardian.
- Transfer personal data to another country:
  - unless we have provided to the Data Protection Commissioner proof of appropriate safeguards with respect to the protection of the personal data;
  - unless the data subject has given explicit consent to the proposed transfer;
  - the transfer is necessary for the performance of a contract between us and the data subject or the implementation of pre-contractual measures taken at the data subject's request; or
  - in such other circumstances as may be allowed by law.
- Without lawful excuse, disclose personal data in any manner that is incompatible with the purpose for which such data has been collected.

Annex 3

The Data Protection Notice

DATA PROTECTION NOTICE

Purpose

In our dealings with you, we are called upon to process your personal data. The purpose of this Data Protection Notice is to explain to you:

1. Who we are and how we may be contacted;
2. The categories of personal data we collect;
3. The purpose for which we collect your personal data and the lawful basis for such collection;
4. The intended recipients of the personal data;
5. Whether the supply of personal data is voluntary or mandatory;
6. Your rights relating to your personal data being processed by us;
7. The possible existence of automated decision making in respect of your personal data;
8. The period for which we will store your personal data;
9. Whether, and in what circumstances, we may transfer your personal information to another country, and the safeguards we have put in place in relation to such transfer; and
10. How we conduct direct marketing.

Application

This Data Protection Notice applies to any processing of your personal information by us, whether such information is provided to us through our website, by email, through the filling of forms (including employment-related ones), through the exchange of contractual documents, by letter or fax, verbally, or through any other means.

By entering into a business relationship with us, or by providing your personal data to us, you confirm that you are agreeable to the processing of your personal data in accordance with the terms of this Data Protection Notice.

Technical terms

We have tried to use simple and plain English as far as possible in this Data Protection Notice. However, data protection is a complex subject and the use of technical terms from time to time is inevitable. We have therefore set out below definitions of the technical terms we have used in this document:

*"**Personal data**": Any data which allows or could allow us to identify you.*

*"**Processing**": Any manipulation of personal data, including 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.*

1. Who we are and how we may be contacted

Details about us and how we may be contacted are set out in the table found in the schedule of this Data Protection Notice (the **"Information Table"**).

We have appointed a Data Protection Officer to monitor the adherence to data protection principles within our organisation. His name and contact details are also set out in the Information Table. You may wish to contact him if you have any query regarding this Data Protection Notice or any other matter relating to your personal data.

2. The categories of personal data we collect

2.1. Categories

The categories of personal data we collect are set out in the Information Table.

While we have attempted to make the list as exhaustive as possible, there is a possibility we may have omitted come categories due to the complexity of our organisation and the intricacies of our operations.

We encourage you to get in touch with our Data Protection Officer if you find that any of your personal data which we collect is not listed in this Data Protection Notice. We will then endeavour to promptly amend this Data Protection Notice accordingly.

2.2. Personal data of children

We do not knowingly process data relating to a child under the age of 16, without the consent of his parents or guardians. If you are a child under the age of 16, please ensure that you (a) obtain the consent of your parents or guardians before providing such data to us; and (b) provide a record of such consent to us.

If you provide us with the personal data of another person, you are responsible for ensuring that such person is made aware of the information contained in this Data Protection Notice and that the person has given you his consent for sharing his personal data with us.

2.3. Special categories of personal data

Special categories of personal data are data pertaining to racial or ethnic origin, political opinion or adherence, his religious or philosophical beliefs, membership of a trade union, physical or mental health or condition, sexual orientation, practices or preferences, genetic data or biometric data uniquely identifying someone or data relating to the commission or alleged commission of an offence.

We do not collect any of your personal data which falls within the special categories of personal data, unless:

(a) you have consented to the processing for one or more specified purposes;
(b) the processing is necessary:
    (i) for the performance of a contract to which you are a party or in order to take steps at your request before entering into a contract;
    (ii) for compliance with any legal obligation to which we are subject;
    (iii) for the purpose of historical, statistical or scientific research; or
    (iv) for such other legitimate purposes as may be authorised by law.

The special categories of data which we may collect, in accordance with the above terms, are set out in the Information Table.

2.4. Cookies

Please note that we collect information via cookies and other similar technologies (such as web beacons).

Cookies are small text files that are automatically placed on your computer or mobile device when you visit a website. They are stored by your internet browser. Cookies contain basic information about your use of the internet. Your browser sends these cookies back to our website every time you visit it, so it can recognise your computer or mobile device and personalise and enhance your browsing experience.

We invite you to read our **Cookie Policy** if you wish to further understand our use of cookies in relation to your personal data.

3. The purpose for which we collect personal data and the lawful basis for such collection

3.1. Purpose

We collect personal data for a number of purposes, including:

(a) to provide services to our clients. You will find a brief description of the services we provide in the Information Table;
(b) to enter into contractual relationships with suppliers and service providers and execute such contracts;
(c) to keep a database of clients and potential clients to communicate with in respect of our services and matters related thereto;
(d) to comply with our legal obligations towards authorities, including the Mauritius Revenue Authority, the Registrar of Companies and the regulators;
(e) to keep a database of candidates who have sent CVs to us, for potential future use;
(f) to keep appropriate employment-related information on employees;
(g) to provide facilities and benefits to our employees;
(h) for security purposes;
(i) to generate statistics and reports on different aspects of our business; and
(j) for such other purposes as may be related, directly or indirectly, to our business activities.

3.2. Lawful basis

The law (a) provides that we cannot process personal data unless we have a lawful basis for such processing; and (b) lists a number of lawful bases for the processing of data.

The lawful bases which apply to our processing of your personal data are as follows:

(a) your consent having been obtained; and/or

(b) the processing being necessary:
    (i) for the performance of a contract to which you are a party or in order to take steps at your request before entering into a contract with you; and/or
    (ii) for compliance with any legal obligation to which we are subject; and/or
    (iii) for the purpose of historical, statistical or scientific research; and/or
    (iv) for the legitimate interests pursued by us (except if the processing is unwarranted in any particular case having regard to the harm and prejudice to your rights and freedoms or legitimate interests).

4. The intended recipients of the personal data

The primary purpose of collecting your personal data is for our own uses, in connection with our business relationship with you. In this context, we may disclose your personal information to our collaborators, including our employees, consultants, advisors, directors and service providers who need to access the personal data.

However, we may also be required to disclose your personal data to third parties to comply with our legal obligations. Such third parties may include the Registrar of Companies, the Mauritius Revenue Authority, the Stock Exchange of Mauritius Ltd, the Financial Services Commission and other government authorities.

As you are aware, we form part of the Rogers Group. In this context, we may, from time to time, disclose your personal information to other companies forming part of the Rogers Group. The objective of this disclosure is to develop a centralised database of clients, which would help the Rogers Group better identify your needs and provide tailor-made packages and services to you. If you do not wish that your personal data be communicated to other companies within the Rogers Group, we encourage you to notify our Data Protection Officer as soon as possible.

5. Whether the supply of personal data is voluntary or mandatory

The provision of personal data is of course entirely voluntary. You are free to choose whether to provide your personal data to us or not. Please note however that if you choose not to provide your personal data to us, we may not be able to provide certain services to you or enter into a contractual relationship with you.

6. Your rights relating to your personal data being processed by us

The law confers upon you a number of rights relating to the personal data being processed by us. These rights are set out below. If you wish to exercise any of the said rights, we encourage you to contact our Data Protection Officer.

6.1. Right to withdraw consent at any time

Where we process your personal data on the basis of your consent, you may withdraw such consent at any time. The withdrawal of your consent will not affect the lawfulness of any processing done by us prior to such withdrawal.

Please note that withdrawing your consent may result in us not being able to provide certain services to you or enter into a contractual relationship with you.

6.2. Right of access

You may request a copy of the personal data we hold about you. Kindly ensure that such request is made in writing to our Data Protection Officer.

Please note that if, in our opinion, your request is manifestly excessive, we may either not attend to your request or charge a fee for attending to same.

6.3. Rectification, erasure or restriction of processing

You may also, at any time, request:

(a) to have any inaccurate personal data we hold on you corrected. This includes the right to supplement and/or update existing personal data provided to us;

(b) that we erase any personal data we hold on you where (i) such data is no longer necessary in relation to the purpose for which it was collected or otherwise processed; (ii) you have withdrawn your consent to us holding and processing such data and there are no overriding legitimate grounds for the continued processing; or (iii) your personal data has been unlawfully processed.

You will understand that this right is not absolute and that it will not be applicable where the exceptions provided for by law apply, including where our processing of your personal data is necessary for the purpose of historical, statistical or scientific research or for compliance with a legal obligation or for the establishment, exercise or defence of a legal claim;

(c) us to restrict processing of your personal data where (i) the accuracy of your personal data is contested by you. This restriction will apply for such period as may be necessary to enable us to verify the accuracy of the data; (ii) we no longer need the personal data for the purpose of processing; (iii) you deem the processing of your personal data to be unlawful, but do not wish us to erase it; or (iv) you have objected to the processing of your data. Such restriction will apply pending verification as to our legitimate grounds to keep processing the personal data, despite your objection.

6.4. Right to object

You have the right to object to our processing of your personal data at any time. Upon receiving such objection, we will stop processing your personal data, except where there are compelling legitimate grounds to continue such processing;

6.5. Right to lodge a complaint

If you feel that we have not processed your personal data lawfully, please do feel free to contact us through our Data Protection Officer.

If you remain unsatisfied, you may lodge a complaint with the Data Protection Commissioner in Mauritius. Her contact details are as follows:

Address: 5th Floor, SICOM Tower, Wall Street, Ebène
Email address: dpo@govmu.org
Phone number: + (230) 460-0253
Fax: + (230) 489-7346

7. The possible existence of automated decision making in respect of your personal data

Unless one of the following exceptions apply, we will not process your personal data in such as way to subject you to a decision which produces legal effects concerning you or which significantly affects, you, based solely on automated processing, including profiling:

(a) where the decision is necessary for entering into, or performing, a contract between us;
(b) where the decision is authorised by a law to which we are subject and which lays down suitable measures to safeguard your rights, freedoms and legitimate interests; or
(c) where the decision is based on your explicit consent.

8. The period for which we will store your personal data

The law provides that where the purpose for keeping any personal data has lapsed, we should destroy the data as soon as reasonably practicable.

We will keep storing your data for as long as is necessary:

(a) for us to fulfil the purposes we collected it for;
(b) for the performance of any contract which may exist between us;
(c) for us to share with you the latest news regarding our organisation and our services;
(d) for us to keep a record of your preferences in order to service you again on future occasions;
(e) for us to satisfy any legal requirement, including statutory reporting obligations;
(f) for the keeping of adequate records for historical, financial or statistical purposes;
(g) for security purposes;
(h) for the prevention of fraud and abuse; and
(i) for us to defend or enforce our rights.

We wish to draw your attention to the fact that the legal prescription period in Mauritius (i.e. the period during which one party may sue another after the happening of an event) is 10 years for non-immovable-property-related matters. Depending on the nature of our relationship with you, we may, in this context, also choose to keep your personal data for at least the legal prescription period in order to be able to defend or enforce our rights.

In some circumstances, we may anonymise your personal data by pseudonymisation or encryption, such that the personal data can no longer be associated with you, for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

9. Whether, and in what circumstances, we may transfer your personal information to another country, and the safeguards we have put in place in relation to such transfer

Please refer to the Information Table.

10. How we conduct direct marketing

You may from time to time receive communication of advertising or marketing material from us ("**Direct Marketing**") if:

(a) you have given your consent;
(b) you asked for a quote or other information on us;
(c) you have, at any time, purchased goods or services from us and have not opted out of receiving advertising or marketing material;
(d) you have entered into a contractual relationship with us; or
(e) you have provided us with your personal data when you entered a competition or registered for a promotion.

You have the right, at any time, to object to the processing of your personal data for direct marketing purposes. Where we receive such an objection from you, we will stop processing your data for direct marketing purposes.

11. Queries

If you have any queries on this Data Protection Notice, we encourage you to get in touch with us through our Data Protection Officer.

Schedule

The Information Table

Who we are	VLH Ltd and the entities which are listed below in Annex A.
Our contact details	**Address:** Village Laboudonnais, Mapou 31803, Mauritius **Telephone number:** +230 266-9700 **Fax number:** +230 266-9797 **Email address:** Valerie.Saillard@vlh.mu
Our Data Protection Officer	Valerie Saillard-Mille Her contact details are the same as above.
The categories of personal data we collect (including the special categories of personal data)	Please refer to Annex B below.
Our services	Please refer to Annex A below for the list of our entities and their corresponding activities.
Transfer of personal data to another country	We endeavour to ensure that whenever we transfer personal data to other countries, the recipients of such personal data comply with all applicable data protection laws and principles.

Annex A

The List of entities that form part of the enterprise

Entity	Business Activity
VLH Ltd	Tourism and hospitality
Veranda Tamarin Ltd	- Wholesale trade - Transport by road - General retailer - Owns hotels - Owns and manages fitness centres - Restaurants (including liquor & other alcoholic beverages) with entertainment - Retail sale of other goods in specialised stores
Heritage Golf Club Ltd	- Wholesale trade - Retail sale of other goods in specialised stores
VLH Training Ltd	- Training Institution / (Education)
Seven Colours Spa Lt	- Distributor of general merchandise - Tourism
Heritage Events Co Ltd	- Business/Professional and Management Consultancy Service (including medical and para-medical practitioners and optician)(Firm)

Annex B

The categories of personal data we hold

Categories of personal data	Examples
Identity	- First name - Maiden name - Last name - Username or similar identifier - Marital status - Job title - Date of birth - Gender - Signature
Contact details	- Email Address - Telephone numbers - Fax numbers - Address - Country - City - Postal code
Financial	- Credit/Debit card numbers - Payment card details (including security code numbers) and other related billing information - Bank details - Payment card details
Transactional	- Payments to and from you - Services/goods purchase history
Technical	- Internet Protocol (IP) address - Login data - Browser type and version - Time zone setting and location - Browser plug-in types and versions - Operating system and platform - Other technology on the devices used to access our website - Traffic data - Media Access Control (MAC) address - Smartphone Defined User name - Surfing history
Preferences and interests	- Golf - Beach - Family - Wellness - Nature - Adventure - Food - Romance - Wedding

	- Business - Shopping - Culture - Discovery
Usage	- Information about how you use our website and service (You may also wish to consult our **Cookie Policy**).
Additional information we collect if your relationship with us is an HR-related one (solicitation, recruitment or employment)	- Qualifications - CVs - Records of past employment - Employment records, including remuneration details, attendance records, performance-related information - Fingerprints, if we operate a fingerprint-based access systems
Special categories of personal data	- Fingerprints (for the purposes of operating a fingerprint-based access system for employees) - Criminal records, including certificate of character (for HR purposes and to meet our obligations towards the Financial Services Commission) - Trade union membership records (if you are an employee) - Health records (if you are an employee and are or wish to become a member of Rogers Pension Fund or Rogers Group Provident Association)
Others	- Photographs - Videos, including where we operate CCTV surveillance systems

Annex 4

Personal data breach notification form

Personal Data Breach Notification

Under section 25 of the Data Protection Act, in case of a personal data breach[1], the controller[2] shall without undue delay and where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Data Protection Office.

Swift containment and recovery from a personal data breach is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form. If you are waiting for completion of an internal investigation, please tell us.

1. Particulars of controller giving the notification

(a) Name of controller: _____

(b) Address: _____

(c) Is the controller registered with the Data Protection Office(Y/N)? _____

(d) Name of processor[3] where the data breach occurred (if applicable):

_____

(e) Telephone number of controller: _____ Fax number: _____

(f) Email address of controller _____

(g) Name of Designated Data Protection Officer (*Mr./Ms./Mrs):

_____

(*Please delete as appropriate)

(h) Designation: _____

(i) Telephone number: _____

_____

(j) Email address: _____

1

2. Nature of the personal data breach

(a) When did the personal data breach happen?

_____

(b) If there has been a delay (more than 72 after becoming aware of the incident and reporting it to the Data Protection Office), please provide your justifications for the delay:

_____

_____

_____

(c) Describe the personal data breach in as much detail as possible including cause(s)

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

(d) What categories of data subjects[4] are concerned?

(Note: Examples of categories are employees, clients, suppliers, shareholders, etc.)

_____

_____

(e) What is the approximate number of data subjects affected?

_____

(f) Are the affected data subjects aware of the personal data breach?

_____

(g) Has any affected data subject complained to the controller? If so, how many complaints have been received?

_____

(h) What are the categories of personal data records concerned?

Note: Examples of categories are biometric data, genetic data, health data, special categories of personal data[5], financial data, etc.

_____

_____

(i) What is the approximate number of personal data records concerned?

_____

(j) Is there any risk of harm to any affected individual/s? ☐ Yes ☐ No

Please explain below why there is / there is no real risk of such harm.

_____

_____

_____

_____

_____

_____

_____

_____

3. Containment and recovery

(a) Describe all measures taken or which will be taken to address the personal data breach

(b) Has the data placed at risk now been recovered? If so, please inform when it occurred.

(c) What measures have or will been taken to mitigate the possible adverse effects of the personal data breach?

(d) Has any assistance been provided or will be provided to affected individuals to help them mitigate the consequences of the data breach?

4. Previous contact with the Data Protection Office in connection with Data Breach Notification.

Has the controller notified any previous data breach to the Data Protection Office in the last 2 years? If so, please provide the date/s and any reference/s.

_____

_____

5. Notification to regulators/law enforcement agencies

Has the controller notified any other regulator/ law enforcement agency/body on the data breach? If so, list the names.

_____

_____

Signature: _____

Name: _____

Title: _____

Date: _____

Send your completed form to: **The Data Protection Commissioner,**
Data Protection Office,
5th Floor, SICOM Tower
Wall Street, Ebène
Republic of Mauritius

Notes

1. **Personal data breach** means 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.
2. **Controller** means 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.
3. **Processor** means a person who, or public body which, processes personal data on behalf of a controller.
4. **Data subject** means 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.
5. **Special categories of personal data** in relation to a data subject, means personal data pertaining to (a)his racial or ethnic origin;(b)his political opinion or adherence;(c)his religious or philosophical beliefs;(d)his membership of a trade union;(e)his physical or mental health or condition;(f)his sexual orientation, practices or preferences;(g)his genetic data or biometric data uniquely identifying him;(h)the commission or alleged commission of an offence by him;(i)any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any Court in the proceedings; or (j)such other personal data as the Commissioner may determine to be sensitive personal data.

Annex 5

Security and organisational measures

1. Physical measures

1.1. Offices and storage units, including filing cabinets and compactors, should, as far as possible, be kept locked.

1.2. Server rooms should, as far as possible, be kept locked.

1.3. The use of safes should be considered.

1.4. Employees should adopt a “clean desk” policy, and in particular:

1.4.1. think twice before making a physical copy of a document and if they do make a copy, to securely destroy it afterwards;
1.4.2. not write passwords down;
1.4.3. lock away devices (e.g. computers, laptops, phones and iPads) and make sure they are password-protected or encrypted; and
1.4.4. as far as possible, keep documents containing personal information locked in their drawers and lockers.

1.5. There should, as far as possible, be 24-hour security throughout the building, and it should be ensured that burglar alarms and fire alarms are in place.

1.6. The use of CCTV cameras should be considered where appropriate.

1.7. A memo should be sent to all employees to remind them of the above matters.

2. IT measures

As set out in any IT or Information Security Policy adopted by Rogers and Company Ltd for the Group from time to time.

3. Organisational Measures

3.1. Regular training sessions should be conducted with employees to remind them of the principles applicable to the processing of personal data and their duties relating thereto. A record of such training sessions should be maintained by the Data Protection Officer.

3.2. All new contracts of employment should contain a clause of confidentiality and a clause relating to the manner in which personal data should be processed.

3.3. All new contracts with third parties with whom personal data is shared should contain a clause of confidentiality and a clause relating to the manner in which personal data should be processed.

3.4. There should be regular audits of compliance with the Manual.

Annex 6

Data Protection Impact Assessment Form

Data Protection Impact Assessment Form		
	To be filled-in by Management	**Comments of Data Protection Officer**
Date		
Name of organisation		
Name of person conducting the assessment		
Title		
Systematic description of the envisaged processing operations		
The purposes of the processing, including, where applicable, the legitimate interest pursued by the organisation		
Assessment of the necessity of the processing operations in relation to the purposes		
Assessment of the risks to the rights and freedoms of data subjects		
Assessment of the proportionality of the processing operations in relation to the purposes on the one hand and the risks to the rights and freedoms of data subjects on the other hand		
Measures envisaged to address the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Act, taking into account the rights and legitimate interests of data subjects and other persons concerned.		

Annex 7

Access to personal data (information to be provided to data subject)

1. The purpose of the processing
2. The categories of personal data concerned
3. The recipients or categories of recipient to whom the data have been or will be disclosed
4. The period for which the data will be stored or, if this is not possible, the criteria used to determine that period
5. The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to the processing of the data
6. The right to lodge a complaint with the Data Protection Commissioner
7. Where the personal data are not collected from the data subject, any available information as to their source
8. The existence of automated decision making, including profiling, and information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject
9. Appropriate safeguards taken in case the personal data are transferred or intended to be transferred to another country.

Note: Most of the information set out above will be found in the Data Protection Notice and the may refer the data subject to the relevant parts of the Data Protection Notice in respect of such information.

Annex 8

Data Protection Register

Data Protection Register **VLH Ltd and all entities listed in Annex 1 of the Data Protection Compliance Manual** **Data Protection Officer:** Valerie Saillard-Mille				
Date	Description of issue	Data subject(s) involved (if applicable)	Measures taken to dealt with the issue	Comments