Contact Harald Privacy Policy

1. Introduction and purpose of this privacy policy

1.1 VT42 Pty Ltd ABN 77 373 551 818 trading as Contact Harald (**Contact Harald, us, we or our**) has developed a Bluetooth enabled card (**Card**) and application called Contact Harald to allow business, healthcare and other organisations (who are our customers) to conduct contact tracing for the purposes of tracing infections of COVID-19 and other communicable diseases.

1.2 This privacy policy sets out how personal information collected by Controllers using our products and services will be handled in accordance with the *Privacy Act 1988* (Cth) (**Privacy Act**) and the *Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements — Public Health Contact Information) Determination 2020* (**Biosecurity Determination**).

1.3 This privacy policy outlines how we comply with our obligations under the Privacy Act regarding the collection, use, disclosure, storage, security and access of your personal information.

1.4 We reserve the right to vary this policy from time to time (at our sole discretion). If we make such a variation, the updated policy will be posted on our website and will apply to all personal information that we hold at the time of variation. Your continued use of our website, Card or services after any change in this privacy policy will constitute your acceptance of such change.

2. Our Cards and End User personal information

2.1 We provide a service to our customers whereby it is the customer who distributes, manages and controls Cards and personal information (known in this policy as a "**Controller**") for its end users such as you (**End Users**).

2.2 By way of example, a customer of ours will operate a business and procure our products and services for the benefit of its End Users who may be its employees, contractors and visitors (who will carry Cards). The customer will be the Controller who will decide who is given a Card, the rules for using the Cards (in respect of the Controller's operations) and how to manage Cards. These are matters which we do not control.

2.3 To use the Card, each End User will give its Controller personal information which the Controller will access and manage including uploading such information to the cloud run by a third party cloud provider that we have engaged for the Controller. It is then for the Controller to maintain and update such information in the cloud, and providing access to such information and ensuring it is accurately and securely kept for the End User.

2.4 We do not manage nor can we access your personal information in the cloud unless we are given consent via the relevant Controller.

2.5 When an infection is discovered and how notifications and communications are handled are all matters for the Controller and the End User. These are matters out of our control because:

(a) the Controller is responsible and liable for the collection and management of the personal information belonging to End Users; and

(b) whether the Controller and/or the End User are responsible for notifying health authorities and complying with their directions is a matter for local law.

2.6 Contact Harald does not use geolocation data. No personal information is stored on the Card that the end user carries around other than the unique card identification number so that the card can be later linked to you by your Controller.

2.7 The data that is stored on the Card is limited to recording or "tracing" close contact interactions between two or more Contact Harald Cards detected within 2 metres proximity of each other for a period of 2 minutes or longer. Each Card is designed to store 20 days of proximity contacts.

3. End User acknowledgement

3.1 By registering for a Card, giving your details to a Controller or by using a Card, you have agreed and consented to:

(a) your relevant Controller being the entity responsible and liable for handling your personal information, not us;

(b) your relevant Controller using your personal information subject to:

(i) the Controller's privacy policy; and

(ii) the laws applicable to the jurisdiction the Controller is subject to;

(c) where we have received consent via the Controller, a health authority has compelled us or we have a legal reason as provided for in this privacy policy, Contact Harald using your personal information in accordance with this privacy policy; and

(d) Contact Harald collecting the data from the Card via Bluetooth, keeping it on a secure cloud database server and using it in accordance with this privacy policy.

3.2 We may also collect your personal information from your Controller for the purpose of assisting:

(a) the Controller or the End User (or both); and/or

(b) health authorities and health service providers.

4. Types of personal information the Controller will collect

4.1 For our customers (i.e. the Controller) to provide the Card to End Users (for their designated purpose) and to support their use, including for Controllers and End Users to communicate with each other regarding such use and the reporting of infections (which is out of our control and we do not do), the Controller will collect personal information including but not limited to:

(a) End User full name (or pseudonym if permitted by the Controller's privacy policy) should the need to be contacted arise;

(b) End User mobile phone numbers (so that the End User can be contacted if needed for contact tracing);

(c) End User home phone numbers (as an alternative contact method for the End User if needed for contact tracing); and

(d) End User email addresses (as an alternative contact method for the End User if needed for contact tracing).

4.2 What the Controller does with such information is:

(a) subject to the Controller's privacy policy and laws applicable to the jurisdiction the Controller is in; and

(b) the responsibility and full liability of the Controller.

4.3 Generally, personal information provided by End Users that is uploaded to the cloud (via the Controller) will be de-identified, securely stored in the Contact Harald cloud server on a protected and encrypted basis.

5. Unsolicited collection of personal information

5.1 If we receive unsolicited personal information, we will, as soon as practicable, destroy, delete or de-identify the personal information if it is lawful and reasonable for us to do so.

6. Contact Harald's Use of personal information

6.1 We do not sell, rent or trade personal information to third parties and will only disclose personal information to a third party:

(a) who is a Controller;

(b) who is a relevant health authority or service provider;

(c) where the disclosure is consistent with this privacy policy;

(d) the End User has consented (including implicitly consented by giving your contact details to be sent elsewhere); or

(e) the disclosure is required or authorised at law, by a court order, or by a decision of a government agency or department.

6.2 Although we do not manage personal information, where we assist a Controller or an End User we will primarily use and/or disclose personal information for the following purposes:

(a) to supply and support our products and services (and provide information in respect of such);

(b) for public health purposes (including disclosures to health authorities and health providers);

(c) to allow our customers (your Controller) to maintain an online account with us, and so that we can communicate effectively with our customers (for example by email in relation to the customer account and orders);

(d) for usual account keeping and record keeping purposes;

to carry out our obligations and enforce our rights arising from any contracts entered into between our customers and us, including for billing and collections; and

(e) as stated elsewhere in this policy or any other agreement we may have with you.

6.3 In any event, we may also disclose your personal information where a “permitted general situation” exists as defined in the Privacy Act, such as:

(a) use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual or to public health or safety and it is unreasonable or impracticable to obtain consent;

(b) we have reason to suspect that unlawful activity or misconduct of a serious nature has been (or may be) engaged in and use or disclosure is necessary in order for us to take appropriate action;

(c) use or disclosure is reasonably necessary for the establishment, exercise or defense of a legal or equitable claim; or

(d) use or disclosure is reasonably necessary for a confidential alternative dispute resolution process. This may be the case where the counter party to your transaction is based overseas.

7. What happens when there is a positive test result

7.1 In the event that an End User tests positive for an infection, the relevant Controller will use the stored personal contact information to notify you and enable notification to people who have recorded close contact within the previous 20 days. Once an infection is known, it is for the Controller and/or End Users to notify those who the infected has been in proximity to. Controllers notification may be in various forms, including in person, by telephone, via SMS and/or email alert and may contain advice on next steps as required by the relevant authority for the jurisdiction in which the End User is located. The content of the notifications is a matter for the Controller as we do not control or have input into this process.

7.2 There may be a requirement for your Controller to provide registration information and contact data to health officials to enable wider contact tracing and ensure compliance. This is a matter for the Controller and the relevant laws of the jurisdiction in which the End User is located.

7.3 The use and management of Cards is not for us to act on as we are not responsible or liable for distributing to End Users or managing the use of the Cards. We will not necessarily receive notification of a positive infection result (as that is a matter for the End User and Controller).

8. Overseas disclosures

8.1 Personal information may be kept in the cloud in a jurisdiction where the Controller resides, the End User resides or in a jurisdiction foreign to both. By registering for a Card, giving your details to a Controller or by using a Card, you have agreed and consented to this.

8.2 We have no control over the cloud being located where End Users reside as we do not manage End Users or deal with their personal information.

8.3 We mitigate the risk associated with sending data into the cloud in jurisdictions outside of Australia or outside where the Controller resides by:

(a) taking reasonable steps to ensure that the cloud provider employs industry standard levels of information protection;

(b) requiring a commitment from our cloud providers that they will not use information for a purpose other than for the purpose it was collected and provided to them (including that they must not use for on-selling, disclose for an unrelated purpose or for direct marketing purposes); and

(c) the cloud provider giving a commitment or warranty that it is substantially compliant with:

(i) the privacy legislation with which it is required to comply which has the effect of protecting personal information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect personal information; or, in the alternative

(ii) the Australian Privacy Principles.

8.4 We may also provide your personal information to overseas recipients where:

(a) we are required or authorised by law to do so; or

(b) we suspect that unlawful activity or misconduct of a serious nature is being or may be engaged in.

9. Mailouts and direct marketing

9.1 We do not use End User personal information for direct marketing or mail-outs to End Users.

9.2 Our customers may receive correspondence from us even if they opt-out of receiving marketing material. We will do so where such communications include product maintenance and support information. If this remains an issue, please contact us directly.

10. Security of personal information

10.1 We take reasonable steps to protect End User personal information from misuse, interference, loss, or unauthorised disclosure. We do this by engaging third party cloud service providers and third party security providers, and from time to time we will monitor and review their information security for currency with industry standards however we will not be responsible for data security as:

(a) it is the Controller’s responsibility to upload, maintain and download End User data to and from the cloud;

(b) we cannot access End User data on the cloud without first receiving consent from the Controller or having a lawful reason for such access;

(c) the Controller is responsible for account access and login information, including passwords.

10.2 Where it is no longer required for record keeping purposes or the customer (who is the Controller) has ended its relationship with us, we may destroy or delete data stored on the servers we pay for (unless we are otherwise required or authorised by law to retain it).

11. Accessing and correcting your personal information

11.1 If you are an End User who wishes to access or correct your personal information that you have given, please contact the Controller as they are the administrator of your Card. Your request will be subject to the Controller's privacy policy and laws that you have the benefit of as an individual.

11.2 We are unable to access or correct the End User's personal information without receiving consent via the Controller or unless compelled to by a relevant government authority.

11.3 If you contact us for access to or for the correction of your personal information, we may refuse the request on the basis that the Controller has not communicated the consent or where the relevant government authority has not compelled us to provide such access or correction.

12. Right to be forgotten

12.1 If the Controller holds the End User's personal information and that End User is an individual in the EU, the End User may ask for it to be removed or deleted where:

(a) it is no longer necessary for the purposes for which it was collected;

(b) the End User withdraws consent and that consent was the legal basis for collection;

(c) the End User objects to the use of his or her personal information for automated decision making;

(d) the End User objects to the use of his or her personal information for marketing purposes;

(e) the End User's personal information is being used unlawfully; or

(f) removal is required or authorised at law, by a court order, or by a decision of a government agency or department.

12.2 However, the End User's request for removal may be refused where the personal information is necessary for:

(a) the exercise of a right to freedom of expression and information;

(b) the Controller or we are to comply with an obligation at law;

(c) the performance of a task carried out in the public interest (including public health); or

(d) for the purpose of a judicial process.

12.3 Please note that the Controller and/or we may anonymise personal information to the extent that it has the actual or practical effect of deleting your personal identifiers, or that we cannot identify it as yours to remove or delete.

13. Controller's obligations to Contact Harald

13.1 This paragraph 13 binds Controllers and each Controller agrees that we may enforce the following against it.

Consent

13.2 If at any time the Controller provides us with personal information about someone other than itself (e.g. an End User), it warrants that it has the relevant individual's explicit consent to provide such information for the purpose specified. The Controller acknowledges that we may require proof of such consent to be given to us.

Responsibility

13.3 The Controller acknowledges that it is responsible and liable for the management of the End User personal information consistent with this privacy policy. What the Controller does with the End User's personal information is the responsibility and full liability of the Controller.

Access and correction requests

13.4 Subject to the laws of the jurisdiction in which the Controller and the End Users are subject to or have the benefit of, the Controller will endeavor to respond to requests for access to personal information within a reasonable period of time and will generally provide the End User with the following:

(a) confirmation of whether personal information is being collected and used (or not);

(b) the purpose/s of collecting and using personal information;

(c) the categories of personal information that it holds about the End User (refer to paragraph 4 of this privacy policy);

(d) the recipients or categories of recipients to whom the personal information has been or will be disclosed to;

(e) the period of time that personal information will be stored (where possible); and

(f) notification of the End User's rights.

13.5 The Controller will take reasonable steps to correct personal information, taking into account the purpose for which it is held, its accuracy, the reasonableness and the relevance of an End User's correction request.

13.6 If the Controller refuses a request for access or a correction, it will give reasons for the refusal and information about the complaint mechanism/s that are available. If personal information the subject of a correction has been disclosed to a third party, the Controller will take reasonable steps to notify the third party of any such correction.

13.7 If accuracy of personal information remains an issue or is contested by the End User, the Controller may (at its option) cease to use it, and/or destroy or delete it. Further, we may destroy or delete it (we cannot access or manage however we can destroy or delete).

14. European Union General Data Protection Regulation (GDPR)

14.1 We offer products and support to customers throughout the world. It may be the case that our customers collect personal data from their End Users who are in the EU.

14.2 As we are not the Controller, we do not monitor the behavior of End Users other than solely to the extent that our Cards may communicate with each other about being in proximity with each other.

14.3 If you are in the EU, and you provide personal data to the Controller managing your Card use, it is your responsibility to notify the Controller managing your Card use as to your location in the EU.

14.4 If you are in the EU, then it is the responsibility of the Controller managing your Card to ensure that its use of your personal data does not infringe on your personal data protection entitlements under the GDPR including managing your right to be forgotten, data portability and objections to

the processing of your data. As we cannot access your personal data without consent, we will not be in a position to assist you with these matters.

14.5 Where it is within our control, we will work to ensure that our use does not infringe your personal data protection entitlements under the GDPR.

15. Cookies

15.1 Our websites use cookies, which are small pieces of information stored by a browser or other application and used to connect your computer with information stored about your online activity, searches, preferences and product purchases. You can disable cookies, but if you do so you may not be able to participate in certain activities and you may limit our ability to tailor promotions and communications to you. Our websites do not control or guarantee the effectiveness of browser-based tools for managing cookies.

16. Data breaches

16.1 A data breach can occur as a result of a system fault, human error, or a malicious or criminal attack. When we suffer a data breach that causes individuals to be at risk of serious harm (which we cannot prevent with remedial action) or poses a high risk to your rights and freedoms, we are committed to notifying the regulator and notifying individuals as soon as required by law.

16.2 Our notification/s will include the steps we are taking to resolve the issue and the recommendations about the steps the affected individuals should take in response to the data breach.

17. Making a complaint

17.1 If you have a complaint to make regarding your privacy in respect of the Card, we ask that you first make a complaint to the Controller who gave you the Card (and is responsible for the management of it).

17.2 If you think we have failed to comply with our privacy obligations in respect of the Card, we will ask that you contact us. We will acknowledge your complaint in a prompt manner and give you an estimated timeframe for our response. We are committed to dealing with your complaint in a reasonable and effective manner.

17.3 If we are unable to resolve your complaint or if you are unhappy with the outcome, you may lodge a complaint with the Australian Information Commissioner (www.oaic.gov.au).

18. Contact us

18.1 If you have any questions about this policy, please contact us at privacy@contactharald.com.

This policy was last updated [6 July 2020].