



Privacy Policy

Issued by the Board of Day1 Exchange Pty Ltd

ACN: 656 508 815

Date Updated: October 2022

Contents

Section A – Introduction	
1. Introduction	1
2. When does this policy apply?	1
3. Glossary	1
Section B – Consideration of personal information privacy	2
4. Privacy statement	2
Section C – Collection of personal information (solicited personal information)	2
5. Personal information (other than sensitive information)	2
6. Sensitive information	3
7. Means of collection	3
8. Information collected by day1 exchange	3
9. Purpose of collection	3
Section D – Collection of personal information (unsolicited personal information)	3
10. Dealing with unsolicited personal information	3
Section E – Notification of the collection of personal information	4
11. Notification of collection	4
Section F – Use or disclosure of personal information	4
12. Use or disclosure	4
13. Who does day1 exchange disclose personal information to?	5
Section G – Direct marketing	5
14. Direct marketing	5
15. Exception – personal information other than sensitive information	5
16. Exception – sensitive information	6
17. Requests to stop direct marketing	6
Section H – Cross border disclosure of personal information	6
18. Disclosing personal information to cross border recipients	6

Contents

Section I – Adoption, use or disclosure of government identifiers	6
19. Adoption of government related identifiers	6
20. Use or disclosure of government related identifiers	7
Section J – Integrity of personal information	7
21. Quality of personal information	7
22. Security of personal information	7
23. Storage of personal information	7
Section K – Access to, and correction of, personal information	7
24. Access	7
25. Exceptions	8
26. Refusal to give access	8
Section L – Correction of personal information	8
27. Correction of information	8
28. Refusal to correct information	8
29. Request from a client to associate a statement with their information	9
30. Dealing with requests	9
Section M – Making a privacy complaints	9
31. Complaints	9
Section N – Miscellaneous	10
32. Notifiable data breaches scheme	10
33. Policy breaches	10
34. Retention of forms	10
35. Policy review	10

Section A – Introduction

1. Introduction

- 1.1 As part of Day1 Exchange Pty Ltd’s (“Day1 Exchange”) process to ensure that it continues to maintain the highest levels of professional integrity and ethical conduct, Day1 Exchange has adopted this Privacy Policy (“Policy”) to manage personal information in an open and transparent manner.
- 1.2 The provisions of this Policy assist Day1 Exchange in complying with the requirements of the Privacy Act 1988 (Cth) (“Privacy Act”) and the Australian Privacy Principles in protecting the personal information Day1 Exchange holds about its clients.

2. When does this policy apply?

- 2.1 This Policy applies to all representatives and employees of Day1 Exchange at all times and the requirements remain in force on an ongoing basis.

3. Glossary

Term	Definition
APP entity	Means an agency or organisation as defined in section 6 of the Privacy Act.
Australian law	Means a) an Act of the Commonwealth or of a State or Territory; or b) regulations, or any other instrument, made under such an Act; or c) a Norfolk Island enactment; or d) a rule of common law or equity.
Collects	Day1 Exchange collects personal information only if Day1 Exchange collects the personal information for inclusion in a record or generally available publication.
Court/tribunal order	Means an order, direction or other instrument made by: a) a court; or b) a tribunal; or c) a judge (including a judge acting in a personal capacity) or a person acting as a judge; or d) a magistrate (including a

Term	Definition
	magistrate acting in a personal capacity) or a person acting as a magistrate; or e) a member or an officer of a tribunal; and includes an order, direction or other instrument that is of an interim or interlocutory nature.
De-identified	Personal information is de-identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.
Eligible Data Breach	An eligible data breach occurs: a) when there has been unauthorised access or unauthorised disclosure of personal information, or a loss of personal information, that Day1 Exchange holds; and b) the unauthorised access or unauthorised disclosure is likely to result in serious harm to one or more clients; and c) Day1 Exchange is not able to prevent the likely risk of serious harm with remedial action.
Holds	Day1 Exchange holds personal information if it has possession or control of a record that contains the personal information.
Identifier of an individual	Means a number, letter or symbol, or a combination of any or all of those things, that is used to identify the individual or to verify the identity of the individual, but does not include: a) the individual’s name; or b) the individual’s ABN (within the meaning of the A New Tax System (Australian Business Number) Act 1999); or c) anything else prescribed by the regulations.
Permitted general situation	As defined in s16A of the Privacy Act.
Permitted health situation	As defined in s16B of the Privacy Act.

Term	Definition
Personal information means	Means information or an opinion about an identified individual, or an individual who is reasonably identifiable: <ol style="list-style-type: none"> a) whether the information or opinion is true or not; and b) whether the information or opinion is recorded in a material form or not.
Sensitive information	Means <ol style="list-style-type: none"> a) information or an opinion about an individual's: <ol style="list-style-type: none"> 1) racial or ethnic origin; or 2) political opinions; or 3) membership of a political association; or 4) religious beliefs or affiliations; or 5) philosophical beliefs; or 6) membership of a professional or trade association; or 7) membership of a trade union; or 8) sexual orientation or practices; or 9) criminal record; that is also personal information; or b) health information about an individual; or c) genetic information about an individual that is not otherwise health information. d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or e) biometric templates.

b) contains the following information:

- 1) the kinds of personal information that Day1 Exchange collects and holds;
 - 2) how Day1 Exchange collects and holds personal information;
 - 3) the purposes for which Day1 Exchange collects, holds, uses and discloses personal information;
 - 4) how an individual may complain about a breach of the Australian Privacy Principles, or other relevant legislation that binds Day1 Exchange, and how Day1 Exchange deals with such a complaint;
 - 5) whether Day1 Exchange is likely to disclose personal information to overseas recipients; and
 - 6) if Day1 Exchange is likely to disclose personal information to overseas recipients, the countries in which such recipients are likely to be located if it is practicable to specify those countries in this policy.
- 4.3 Day1 Exchange ensures that the Day1 Exchange's Privacy Statement is available free of charge and in such form as appropriate. Day1 Exchange makes the Privacy Statement available on its website.
- 4.4 If the Privacy Statement is requested in a particular form, Day1 Exchange will take such steps as are reasonable to provide the Privacy Statement in the form requested.

Section C – Collection of personal information (solicited personal information)

5. Personal information (other than sensitive information)

- 5.1 This Section C applies to the collection of personal information that is solicited by Day1 Exchange.
- 5.2 Day1 Exchange does not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of Day1 Exchange's functions or activities.
- 5.3 Day1 Exchange's functions or activities include operating as a digital currency exchange registered with the Australian Transaction Reports and Analysis Centre ("AUSTRAC").

Section B – Consideration of personal information privacy

4. Privacy statement

- 4.1 Day1 Exchange's Directors ensures that at all times the provisions of this policy are implemented in the day to day running of Day1 Exchange.
- 4.2 The Directors ensure that at all times this Policy:
 - a) is current and reflects the latest applicable Australian laws; and

6. Sensitive information

- 6.1 Day1 Exchange does not collect sensitive information about an individual unless:
- a) the individual consents to the collection of the information and the information is reasonably necessary for one or more of Day1 Exchange's functions or activities (as described in section 5.3); or
 - b) the collection of the information is required or authorised by or under an Australian law or a Court/Tribunal order; or
 - c) a permitted general situation exists in relation to the collection of the information by Day1 Exchange; or
 - d) a permitted health situation exists in relation to the collection of the information by Day1 Exchange.

7. Means of collection

- 7.1 Day1 Exchange only collects personal information by lawful and fair means.
- 7.2 Day1 Exchange only collects personal information about an individual from the individual (rather than someone else), unless it is unreasonable or impracticable to do so or the individual has instructed Day1 Exchange to liaise with someone else.
- 7.3 Day1 Exchange collects personal information from an individual when:
- a) Day1 Exchange's Application Form is completed;
 - b) a Client provides the information to Day1 Exchange's representatives over the telephone or via email;
 - c) a Client provides the information to Day1 Exchange on the website; e.g.
 - d) a third party (e.g. credit reporting agency) provides Day1 Exchange the personal information for the purposes of Day1 Exchange providing the Client with its services.

8. Information collected by day1 exchange

- 8.1 The information Day1 Exchange collects may include the following:
- a) name;

- b) date of birth;
- c) postal or email address; or
- d) phone numbers;
- e) other information Day1 Exchange considers necessary to their functions and activities.

9. Purpose of collection

- 9.1 If an individual is acquiring or has acquired a service from Day1 Exchange, the individual's personal information will be collected and held for the purposes of:
- a) checking whether an individual is eligible for Day1 Exchange's service;
 - b) providing the individual with Day1 Exchange's service;
 - c) managing and administering Day1 Exchange's service;
 - d) protecting against fraud, crime or other activity which may cause harm in relation to Day1 Exchange's services;
 - e) complying with legislative and regulatory requirements in any jurisdiction; and
 - f) to assist Day1 Exchange in the running of its business.
- 9.2 Day1 Exchange may also collect personal information for the purposes of letting an individual know about services that might better serve their needs or other opportunities in which they may be interested. Please refer to Section G for further information.

Section D – Collection of personal information (unsolicited personal information)

10. Dealing with unsolicited personal information

- 10.1 If Day1 Exchange:
- a) receives personal information about an individual; and
 - b) the information is not solicited by Day1 Exchange
- Day1 Exchange must, within a reasonable period after receiving the information, determine whether or not it was permitted to collect the information under Section C above.

10.2 Day1 Exchange may use or disclose the personal information for the purposes of making the determination under paragraph 10.1.

10.3 If Day1 Exchange:

a) determines that it could not have collected the personal information; and

b) the information is not contained in a Commonwealth record,

Day1 Exchange must as soon as practicable, destroy the information or ensure that the information is de-identified, only if it is lawful and reasonable to do so.

Section E – Notification of the collection of personal information

11. Notification of collection

11.1 This section 11 applies to:

a) solicited information; and

b) unsolicited information to which section 10 does not apply.

11.2 Day1 Exchange must notify the individual of the following matters in the Privacy Statement:

a) Day1 Exchange's identity and contact details;

b) if Day1 Exchange collects the personal information from a third party or the individual is not aware that Day1 Exchange has collected the personal information, the fact that Day1 Exchange so collects, or has collected the information and the circumstances of that collection;

c) if the collection of the personal information is required or authorised by or under an Australian law or a Court/Tribunal order, the fact that the collection is so required or authorised (including the details of the law or court);

d) the purposes for which Day1 Exchange collects the personal information;

e) the main consequences (if any) for the individual if the information is not collected by Day1 Exchange;

f) any other entities to which Day1 Exchange usually discloses personal information of the kind collected by Day1 Exchange;

g) that Day1 Exchange's Privacy Statement and this Privacy Policy contains information about how the individual may access the personal information about the individual that is held by Day1 Exchange and seek correction of such information;

h) that Day1 Exchange's Privacy Statement contains information about how the individual may complain about a breach of the Australian Privacy Principles and how Day1 Exchange will deal with such a complaint;

i) whether Day1 Exchange discloses the personal information to overseas recipients; and

j) if Day1 Exchange discloses the personal information to overseas recipients – the countries in which such recipients are located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Section F – Use or disclosure of personal information

12. Use or disclosure

12.1 Where Day1 Exchange holds personal information about an individual that was collected for a particular purpose ("the primary purpose"), Day1 Exchange must not use or disclose the information for another purpose ("the secondary purpose") unless:

a) the individual has consented to the use or disclosure of the information; or

b) the individual would reasonably expect Day1 Exchange to use or disclose the information for the secondary purpose and the secondary purpose is:

1) directly related to the primary purpose (if the information is sensitive information); or

2) related to the primary purpose (if the information is not sensitive information);

c) the use or disclosure of the information is required or authorised by or under an Australian law or a Court/Tribunal order; or

d) a permitted general situation exists in relation to the use or disclosure of the information by Day1 Exchange; or

e) Day1 Exchange reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

12.2 Where Day1 Exchange uses or discloses personal information in accordance with section 12.1(e), Day1 Exchange keeps a copy of this disclosure (e.g.: the email or letter used to do so).

12.3 This section 12 does not apply to:

a) personal information for the purposes of direct marketing; or

b) government related identifiers.

12.4 If Day1 Exchange collects personal information from a related body corporate, this section 12 applies as if Day1 Exchange's primary purpose for the collection was the primary purpose for which the related body corporate collected the information.

13. Who does day1 exchange disclose personal information to?

13.1 Day1 Exchange may disclose personal information collected from clients and prospective clients to the following:

a) organisations involved in providing, managing or administering Day1 Exchange's service such as third-party suppliers, e.g. printers, posting services, and our advisers;

b) organisations involved in maintaining, reviewing and developing Day1 Exchange's business systems, procedures and infrastructure, including testing or upgrading Day1 Exchange's computer systems;

c) organisations involved in a corporate re-organisation;

d) organisations involved in the payments system, including financial institutions, merchants and payment organisations;

e) organisations involved in planning and development;

f) other organisations, who jointly with Day1 Exchange's, provide its services;

g) authorised representatives who provide Day1 Exchange's services on its behalf;

h) the individual's representatives, including legal advisers;

i) debt collectors;

j) Day1 Exchange's financial advisers, legal advisers or auditors;

k) fraud bureaus or other organisations to identify, investigate or prevent fraud or other misconduct;

l) external dispute resolution schemes; or

m) regulatory bodies, government agencies and law enforcement bodies in any jurisdiction.

Section G – Direct marketing

14. Direct marketing

14.1 Day1 Exchange must not use or disclose the personal information it holds about an individual for the purpose of direct marketing.

15. Exception – personal information other than sensitive information

15.1 Day1 Exchange may use or disclose personal information (other than sensitive information) about an individual for the purposes of direct marketing if:

a) Day1 Exchange collected the information from the individual; and the individual would reasonably expect Day1 Exchange to use or disclose the information for that purpose; or

b) Day1 Exchange has collected the information from a third party; and either:

1) Day1 Exchange has obtained the individual's consent to the use or disclose the information for the purpose of direct marketing; or

2) it is impracticable for Day1 Exchange to obtain the individual's consent; and

c) Day1 Exchange provides a simple way for the individual to opt out of receiving direct marketing communications from Day1 Exchange;

1) includes a prominent statement that the individual may opt out of receiving direct marketing; or

2) directs the individual's attention to the

fact that the individual may opt out of receiving direct marketing; and
 e) the individual has not made a request to opt out of receiving direct marketing.

16. Exception – sensitive information

16.1 Day1 Exchange may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

17. Requests to stop direct marketing

17.1 Where Day1 Exchange uses or discloses personal information about an individual for the purposes of direct marketing by Day1 Exchange or facilitating direct marketing by another organisation, the individual may request:

- a) that Day1 Exchange no longer provide them with direct marketing communications;
- b) that Day1 Exchange does not use or disclose the individual's personal information for the purpose of facilitating direct marketing by another organisation;
- c) that Day1 Exchange provides the source of the personal information.

17.2 Where Day1 Exchange receives a request from an individual under section 17.1, Day1 Exchange:

- a) gives effect to the request under section 17.1(a) or 17.1(b) within a reasonable period after the request is made and free of charge; and
- b) notifies the individual of the source of the information, if the individual requests it, unless it is impracticable or unreasonable to do so.

17.3 This Section G does not apply to the extent that the following laws apply:

- a) the Do Not Call Register Act 2006;
- b) the Spam Act 2003; or
- c) any other Act of the Commonwealth of Australia.

Section H – Cross border disclosure of personal information

18. Disclosing personal information to cross border recipients

18.1 Where Day1 Exchange discloses personal information about an individual to a recipient who is not in Australia and who is not Day1 Exchange or the individual, Day1 Exchange must ensure that the overseas recipient does not breach the Australian Privacy Principles (with the exception of APP1).

18.2 Section 18.1 does not apply where:

a) Day1 Exchange reasonably believes that:

- 1) information is subject to a law or binding scheme that has the effect of protecting the information in a way that is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and
- 2) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

b) both of the following apply:

- 1) Day1 Exchange has informed the individual that if they consent to the disclosure of information Day1 Exchange will take reasonable steps to ensure the overseas recipient does not breach the Australian Privacy Principles; and
- 2) after being so informed, the individual consents to disclosure;

c) the disclosure of the information is required or authorised by or under an Australian law or a Court/Tribunal order; or

d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1) of the Privacy Act) exists in relation to the disclosure of the information by Day1 Exchange.

Section I – Adoption, use or disclosure of government identifiers

19. Adoption of government related identifiers

19.1 Day1 Exchange must not adopt a government related identifier of an individual as its own identifier unless:

a) Day1 Exchange is required or authorised by or under an Australian law or a Court/Tribunal order to do so; or

b) the identifier, Day1 Exchange and the circumstances of the adoption are prescribed by regulations.

20. Use or disclosure of government related identifiers

20.1 Before using or disclosing a government related identifier of an individual, Day1 Exchange must ensure that such use or disclosure is:

a) reasonably necessary for Day1 Exchange to verify the identity of the individual for the purposes of the organisation's activities or functions; or

b) reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or

c) required or authorised by or under an Australian law or a Court/Tribunal order; or

d) within a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1) of the Privacy Act; or

e) reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

f) the identifier, Day1 Exchange and the circumstances of the adoption are prescribed by regulations.

22.2 Day1 Exchange takes reasonable steps to destroy or de-identify any personal information it holds where:

a) Day1 Exchange no longer needs the personal information for any purpose for which the information may be used or disclosed by Day1 Exchange;

b) the information is not contained in a Commonwealth record;

c) Day1 Exchange is not required to retain that information under an Australian law, or a Court/Tribunal order.

23. Storage of personal information

23.1 Day1 Exchange stores personal information in different ways, including electronically secure data centres that are owned by either Day1 Exchange or external service providers.

23.2 In order to ensure Day1 Exchange protects any personal information it holds from misuse, interference, loss, unauthorised access, modification and disclosure, Day1 Exchange implements the following procedure/system:

a) access to information systems is controlled through identity and access management;

b) employees are bound by internal information securities policies and are required to keep information secure;

c) all employees are required to complete training about information security; and

d) Day1 Exchange regularly monitors and reviews its compliance with internal policies and industry best practice.

Section J – Integrity of personal information

21. Quality of personal information

21.1 Day1 Exchange ensures that the personal information it collects and the personal information it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant.

22. Security of personal information

22.1 Day1 Exchange ensures that it protects any personal information it holds from misuse, interference, loss, unauthorised access, modification and disclosure.

Section K – Access to, and correction of, personal information

24. Access

24.1 Day1 Exchange must give an individual access to the personal information it holds about the individual if so requested by the individual.

24.2 Day1 Exchange must respond to any request for access to personal information within a reasonable period after the request is made.

24.3 Day1 Exchange must give access to the information in the manner requested by the individual, if it is reasonable and practicable to

do so and must take such steps as are reasonable in the circumstances to give access in a way that meets the needs of Day1 Exchange and the individual.

24.4 Day1 Exchange must not charge an individual for making a request and does not impose excessive charges for the individual to access their personal information.

25. Exceptions

25.1 Day1 Exchange is not required to give an individual access to their personal information if:

- a) Day1 Exchange reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or
- b) giving access would have an unreasonable impact on the privacy of other individuals; or
- c) the request for access is frivolous or vexatious; or
- d) the information relates to existing or anticipated legal proceedings between Day1 Exchange and the individual, and would not be accessible by the process of discovery in those proceedings; or
- e) giving access would reveal intentions of Day1 Exchange in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
- f) giving access would be unlawful; or
- g) denying access is required or authorised by or under an Australian law or a Court/Tribunal order; or
- h) Day1 Exchange has reason that unlawful activity, or misconduct of a serious nature, that relates to our functions or activities has been, or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or
- i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
- j) giving access would reveal evaluative information generated within Day1 Exchange in connection with a commercially sensitive decision-making process.

26. Refusal to give access

26.1 If Day1 Exchange refuses to give access in accordance with section 24 or to give access in the manner requested by the individual, Day1 Exchange will give the individual a written notice that sets out:

- a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and
- b) the mechanisms available to complain about the refusal; and
- c) any other matter prescribed by the regulations.

26.2 Where Day1 Exchange refuses to give access under section 25.1(j) Day1 Exchange may include an explanation of the commercially sensitive decision in its written notice of the reasons for denial.

Section L – Correction of personal information

27. Correction of information

27.1 Day1 Exchange must take reasonable steps to correct all personal information, having regard to the purpose for which the information is held where:

- a) Day1 Exchange is satisfied the information is inaccurate, out of date, incomplete, irrelevant or misleading; or
- b) the individual requests Day1 Exchange corrects the information.

27.2 Where Day1 Exchange corrects personal information about an individual that Day1 Exchange previously disclosed to another APP entity and the individual requests Day1 Exchange to notify the other APP entity of the correction, Day1 Exchange must take reasonable steps to give that notification, unless it is impracticable or unlawful to do so.

28. Refusal to correct information

28.1 If Day1 Exchange refuses to correct personal information as requested by the individual, Day1 Exchange will give the individual a written notice that sets out:

- a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

b) the mechanisms available to complain about the refusal; and

c) any other matter prescribed by the regulations.

29. Request from a client to associate a statement with their information

29.1 If:

a) Day1 Exchange refuses to correct personal information as requested by the individual; and

b) the individual requests that Day1 Exchange associate a statement noting that the information is inaccurate, out of date, incomplete, irrelevant or misleading, with the individual's information,

Day1 Exchange must take such steps as are reasonable in the circumstances to associate the statement (as described in section 29.1(b)) with the individual's personal information. The statement is associated with the information in such a way that will make the statement apparent to users of the information.

30. Dealing with requests

30.1 Day1 Exchange:

a) responds to requests under this Section L within a reasonable period after the request is made; and

b) does not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information.

Section M – Making a privacy complaints

31. Complaints

31.1 Day1 Exchange offers a free internal complaint resolution scheme to all customers. Should a client have a privacy complaint, they are to contact Day1 Exchange to discuss their concerns using the following contact details:

a) Email: complaints@day1x.io

b) Post: Level 10, 627 Chapel St, South Yarra VIC 3141

31.2 To assist Day1 Exchange in helping customers, Day1 Exchange asks customers to follow a simple three-step process:

a) gather all supporting documents relating to the complaint;

b) contact Day1 Exchange to review your situation and if possible, resolve your complaint immediately; and

c) if the matter is not resolved to the customer's satisfaction, customers are encouraged to contact Day1 Exchange's Complaints Officer on [insert number] or put their complaint in writing and send it to [insert address].

31.3 Day1 Exchange will rectify any breach if the complaint is justified and takes necessary steps to resolve the issue.

31.4 In certain situations, to deal with a complaint it may be necessary to consult with third parties. However, any disclosure of Personal Information to third parties will be provided with the customer's authority and consent.

31.5 After a complaint has been received, Day1 Exchange sends the customer a written notice of acknowledgement setting out the process. The complaint is investigated, and the decision sent to the customer within thirty (30) days unless the customer has agreed to a longer time. If a complaint cannot be resolved within the agreed time frame or a decision could not be made within thirty (30) days of receipt, a notification will be sent to the customer setting out the reasons and specifying a new date when the customer can expect a decision or resolution.

31.6 If the customer is not satisfied with Day1 Exchange's internal privacy practices or the outcome in respect to complaint, the customer may approach the OAIC with their complaint:

Office of the Australian Information Commissioner

Address: GPO Box 5218, Sydney NSW 2001

Phone: 1300 363 992

Email: enquiries@oaic.gov.au

Website: oaic.gov.au

Section N – Miscellaneous

32. Notifiable data breaches scheme

32.1 Under the Privacy Amendment (Notifiable Data Breaches) Act 2017 (“Privacy Amendment Act”) Day1 Exchange is required to notify the Office of the Australian Information Commissioner (“OAIC”) in relation to all eligible data breaches.

32.2 Day1 Exchange notifies the OAIC by lodging a Notifiable Data Breach Form soon as practicable. The Notifiable Data Breach Form is available at the following link: <https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB>.

32.3 Under the Privacy Amendment Act, Day1 Exchange also promptly informs clients whose personal information has been compromised by the eligible data breach that a breach of their personal information has occurred.

32.4 Day1 Exchange has also developed a Data Breach Response Plan in accordance with the OAIC’s guidelines to ensure the timely notification of all clients affected by any eligible data breach.

33. Policy breaches

33.1 Breaches of this Policy may lead to disciplinary action being taken against the relevant party, including dismissal in serious cases and may also result in prosecution under the law where that act is illegal. This may include re-assessment of bonus qualification, termination of employment and/or fines (in accordance with the Privacy Act).

33.2 Staff are trained internally on compliance and their regulatory obligation to Day1 Exchange. They are encouraged to respond appropriately to and report all breaches of the law and other incidents of non-compliance, including Day1 Exchange’s policies, and seek guidance if they are unsure.

33.3 Staff must report breaches of this Policy directly to the Directors.

34. Retention of forms

34.1 The Compliance Officer retains the completed forms for seven (7) years in accordance with Day1 Exchange’s Document Retention Policy. The completed forms are retained for future reference and review.

34.2 As part of their training, all staff are made aware of the need to practice thorough and up to date record keeping, not only as a way of meeting Day1 Exchange’s compliance obligations, but as a way of minimising risk.

35. Policy review

35.1 Day1 Exchange’s Privacy Policy is reviewed on at least an annual basis by the Compliance Officer of Day1 Exchange, having regard to the changing circumstances of Day1 Exchange. The Compliance Officer then reports to the Director on compliance with this Policy.