



Privacy Policy

Office Number

+612 8330 0850

Email

service@dvmarkets.com



Table of Content

- 4** Section A – Introduction
- 8** Section B – Consideration Of Personal Information Privacy
- 10** Section C – Collection Of Personal Information (Solicited Personal Information)
- 13** Section D – Collection Of Personal Information (Unsolicited Personal Information)
- 14** Section E – Notification Of The Collection Of Personal Information
- 16** Section F – Use Or Disclosure Of Personal Information
- 19** Section G – Direct Marketing
- 22** Section H – Cross Border Disclosure Of Personal Information
- 24** Section I – Adoption, Use Or Disclosure Of Government Identifiers
- 26** Section J – Integrity Of Personal Information
- 28** Section K – Access To, And Correction Of, Personal Information
- 31** Section L – Correction Of Personal Information
- 33** Section M – Miscellaneous

Version Control

Version	Date Updated	Notes
1	4 June 2019	Original document

Introduction



1. Introduction

- 1.1** As part of DV Markets Limited herein referred to as DV Markets) (“**DVM**”) process to ensure that it continues to maintain the highest levels of professional integrity and ethical conduct, DVM has adopted this Privacy Policy (“**Policy**”) to manage personal information in an open and transparent manner.
- 1.2** The provisions of this Policy will assist DVM in complying with the requirements of the Privacy Act and the Privacy Principles in protecting the personal information DVM holds about its clients.

2. When does this policy apply?

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

3. Glossary

■ ***Collects***

DVM collects personal information only if DVM 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 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.

■ ***Holds***

DVM 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 business number

■ ***Personal information means***

means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- 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

- a.* information or an opinion about an individual's:
 - racial or ethnic origin; or
 - political opinions; or
 - membership of a political association; or
 - religious beliefs or affiliations; or
 - philosophical beliefs; or
 - membership of a professional or trade association;
 - membership of a trade union; or
 - sexual orientation or practices; or
 - 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.

End of section A
“Introduction”

Section B

Consideration of personal information privacy



4. Privacy statement

- 4.1** DVM' Compliance Officer ensure that at all times the provisions of this policy are implemented in the day to day running of DVM.
- 4.2** The Compliance Officer must ensure that at all times this Policy:
- a.** is current and reflects the latest applicable laws; and
 - b.** contains the following information:
 - the kinds of personal information that DVM collects and holds;
 - how DVM collects and holds personal information;
 - the purposes for which DVM collects, holds, uses and discloses personal information;
 - how an individual may complain about a breach of the Privacy Principles, or other relevant legislation that binds DVM, and how DVM will deal with such a complaint;

- whether DVM is likely to disclose personal information to overseas recipients;
- if DVM 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 DVM must ensure that the DVM' Privacy Statement is available free of charge and in such form as appropriate. DVM will make the Privacy Statement available on its website.

4.4 If the Privacy Statement is requested in a particular form, DVM will take such steps as are reasonable to provide the Privacy Statement in the form requested.

End of section B

***“Consideration of
personal information privacy”***

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 DVM.
- 5.2** DVM must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of DVM' functions or activities.
- 5.3** DVM' functions or activities include:
- a.** provide financial product advice in derivatives and foreign exchange contracts;
 - b.** deal in financial products including derivatives and foreign exchange contracts;
 - c.** make a market in derivatives and foreign exchange contracts.

6. Sensitive information

- 6.1** DVM must 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 DVM' functions or activities (as described in section 5.3); or
 - b.** the collection of the information is required or authorised by or under an St Vincent and the Grenadines law or a Court/Tribunal order; or
 - c.** a permitted general situation exists in relation to the collection of the information by DVM; or
 - d.** a permitted health situation exists in relation to the collection of the information by DVM.

7. Means of collection

- 7.1** DVM must only collect personal information by lawful and fair means.
- 7.2** DVM must only collect 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 DVM to liaise with someone else.
- 7.3** DVM will collect personal information from an individual when:
- a.** DVM' Application Form is completed;
 - b.** DVM collects and verifies a Client's information to fulfil its obligations under the AntiMoney Laundering and Counter Terrorism Financing Code;
 - c.** a Client provides the information to DVM' representatives over the telephone or via email;
 - d.** a Client provides the information to DVM on the website; and
 - e.** a Client provides the information to DVM via the Client Portal.

8. Information collected by DVM

8.1 The information DVM collects may include the following:

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

9. Purpose of collection

9.1 If an individual is acquiring or has acquired a product or service from DVM, the individual's personal information will be collected and held for the purposes of:

- a. checking whether an individual is eligible for DVM' product or service;
- b. providing the individual with DVM' product or service;
- c. managing and administering DVM' product or service;
- d. protecting against fraud, crime or other activity which may cause harm in relation to DVM' products or services;
- e. complying with legislative and regulatory requirements in any jurisdiction; and
- f. to assist DVM in the running of its business.

9.2 DVM may also collect personal information for the purposes of letting an individual know about products or services that might better serve their needs or other opportunities in which they may be interested. Please refer to Section G for further information.

End of section C

“Solicited personal information”

Section D

Collection of personal information

(unsolicited personal Information)



10. Dealing with unsolicited personal information

10.1 If DVM:

- a.* receives personal information about an individual; and
- b.* the information is not solicited by DVM

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

10.3 If DVM:

- a.* determines that it could not have collected the personal information; DVM 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

12.1 DVM must notify the individual of the following matters in the Privacy Statement:

- a.** DVM' identity and contact details;
- b.** if DVM collects the personal information from a third party or the individual is not aware that DVM has collected the personal information, the fact that DVM 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 St Vincent and the Grenadines 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 DVM collects the personal information;

- e.** the main consequences (if any) for the individual if the information is not collected by DVM;
- f.** any other entities to which DVM usually discloses personal information of the kind collected by DVM;
- g.** that DVM' Privacy Statement and this Privacy Policy contains information about how the individual may access the personal information about the individual that is held by DVM and seek correction of such information;
- h.** whether DVM will disclose the personal information to overseas recipients; and
if DVM discloses the personal information to overseas recipients – the
- i.** countries in which such recipients will be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

End of section E

***“Notification of the collection
of personal information”***

Use or disclosure of personal information



12. Use or disclosure

12.1 Where DVM holds personal information about an individual that was collected for a particular purpose (“the primary purpose”), DVM 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 DVM to use or disclose the information for the secondary purpose and the secondary purpose is:
 - directly related to the primary purpose (if the information is sensitive information); or
 - related to the primary purpose (if the information is not sensitive information);
 - a permitted general situation exists in relation to the use or disclosure of the information by DVM; or
 - DVM 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 DVM uses or discloses personal information in accordance with section 12.1(e), DVM will keep a copy of this disclosure (eg: 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 DVM collects personal information from a related body corporate, this section 12 applies as if DVM' primary purpose for the collection was the primary purpose for which the related body corporate collected the information.

13. Who does dvm disclose personal information to?

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

- a.* organisations involved in providing, managing or administering DVM' product or service such as third party suppliers, e.g. printers, posting services, and our advisers;
- b.* organisations involved in maintaining, reviewing and developing DVM' business systems, procedures and infrastructure, including testing or upgrading DVM' computer systems;
- c.* organisations involved in a corporate re-organisation;
- d.* Organisations that DVM outsources its AML/CTF obligations to, including organisations that conduct background checks;

- e.** organisations involved in the payments system, including financial institutions, merchants and payment organisations;
- f.** organisations involved in product planning and development;
- g.** other organisations, who jointly with DVM', provide its products or services;
- h.** authorised representatives who provide DVM' products or services on its behalf;
- i.** the individual's representatives, including your legal advisers;
- j.** debt collectors;
- k.** DVM' financial advisers, legal advisers or auditors;
- l.** fraud bureaus or other organisations to identify, investigate or prevent fraud or other misconduct;
- m.** external dispute resolution schemes; or
- n.** regulatory bodies, government agencies and law enforcement bodies in any jurisdiction.

End of section F
***“Use or disclosure of
personal information”***

Direct marketing



14. Direct marketing

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

- a.** DVM collected the information from the individual; and the individual would reasonably expect DVM to use or disclose the information for that purpose; or
- b.** DVM has collected the information from a third party; and either:

- DVM has obtained the individual's consent to the use or disclose the information for the purpose of direct marketing; or
 - it is impracticable for DVM to obtain the individual's consent; and
- c.* in each direct marketing communication with the individual DVM:
- includes a prominent statement that the individual may make such a request; or
 - directs the individual's attention to the fact that the individual may make such a request; and
- d.* the individual has not made such a request.

16. Exception – sensitive information

16.1 DVM 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 DVM uses or discloses personal information about an individual for the purposes of direct marketing by DVM or facilitating direct marketing by another organisation, the individual may request:

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

17.2 Where DVM receives a request from an individual under section 17.1, DVM will:

- a.* give 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. notify 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;

b. the Spam Act; or

c. any other Act.

End of section G
“Direct Marketing”

Section H

Cross border disclosure of personal information



18. Disclosing personal information to cross border recipients

- 18.1** Where DVM discloses personal information about an individual to a recipient who is not in St Vincent and the Grenadines and who is not DVM or the individual, DVM must ensure that the overseas recipient does not breach our Privacy Principles.
- 18.2** The countries we may disclose an individual's personal information to include:
- a.** China mainland;
 - b.** Hong Kong; and
 - c.** New Zealand.
- 18.3** Section 18.1 does not apply where:
- a.** DVM reasonably believes that:
 - 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 our Privacy Principles protect the information; and

- 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:
- DVM has informed the individual that if they consent to the disclosure of information DVM will not take reasonable steps to ensure the overseas recipient does not breach our Privacy Principles; and
 - after being so informed, the individual consents to disclosure;
- c.* the disclosure of the information is required or authorised by or under a St Vincent and the Grenadines 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) Privacy Act) exists in relation to the disclosure of the information by DVM.

End of section H

***“Cross border disclosure of
personal information”***

Section I

Adoption, use or disclosure of government identifiers



19. Adoption of government related identifiers

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

- a.** DVM is required or authorised by or under a St Vincent and the Grenadines law or a Court/Tribunal order to do so; or
- b.** the identifier, DVM 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, DVM must ensure that such use or disclosure is:

- a.** reasonably necessary for DVM 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 St Vincent and the Grenadines law or a Court/Tribunal order; or
- d.** within a permitted general situation (other than the situation referred to in 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, DVM and the circumstances of the adoption are prescribed by regulations.

End of section I

***“Adoption, use or disclosure
of government identifiers”***

Section J

Integrity of personal information



21. Quality of personal information

21.1 DVM will ensure 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 DVM will ensure that it protects any personal information it holds from misuse, interference, loss, unauthorised access, modification and disclosure.

22.2 DVM will take reasonable steps to destroy or de-identify any personal information it holds where:

- a.** DVM no longer needs the personal information for any purpose for which the information may be used or disclosed by DVM;
- b.** DVM is not required to retain that information under a St Vincent and the Grenadines law, or a Court/Tribunal order.

23. Storage of personal information

23.1 DVM stores personal information in different ways, including:

- a. hard copy on site at DVMs head office; and
- b. electronically secure data centres owned by either DVM or external service providers

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

- c. access to information systems is controlled through identity and access management;
- d. employees are bound by internal information securities policies and are required to keep information secure;
- e. all employees are required to complete training about information security; and
- f. DVM regularly monitors and reviews its compliance with internal policies and industry best practice.

End of section J
***“Integrity of
personal information”***

Section K

Access to, and correction of, personal information



24. Access

- 24.1** DVM must give an individual access to the personal information it holds about the individual if so requested by the individual.
- 24.2** DVM must respond to any request for access to personal information within a reasonable period after the request is made.
- 24.3** DVM 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 DVM and the individual.
- 24.4** DVM must not charge an individual for making a request, and must not impose excessive charges for the individual to access their personal information.

25. Exceptions

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

- a.** DVM 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 DVM and the individual, and would not be accessible by the process of discovery in those proceedings; or
- e.** giving access would reveal intentions of DVM 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 a St Vincent and the Grenadines law or a Court/Tribunal order; or
- h.** DVM 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
giving access would be likely to prejudice one or more enforcement related
- i.** activities conducted by, or on behalf of, an enforcement body; or
- j.** giving access would reveal evaluative information generated within DVM in connection with a commercially sensitive decision-making process.

25. Refusal to give access

- 26.1** If DVM refuses to give access in accordance with section 24 or to give access in the manner requested by the individual, DVM 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 DVM refuses to give access under section 25.1(j) DVM may include an explanation of the commercially sensitive decision in its written notice of the reasons for denial.

End of section K

***“Access to, and correction of
personal information”***

Correction of personal information



27. Correction of information

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

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

27.2 Where DVM corrects personal information about an individual that DVM previously disclosed to another APP entity and the individual requests DVM to notify the other APP entity of the correction, DVM 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 DVM refuses to correct personal information as requested by the individual, DVM 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.* DVM refuses to correct personal information as requested by the individual; and
- b.* the individual requests that DVM associate a statement noting that the information is inaccurate, out of date, incomplete, irrelevant or misleading, with the individual's information

DVM must take such steps as are reasonable in the circumstances to associate the statement (as described in section 30.1(b)) with the individual's personal information. The statement should be 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 DVM must:

- a.* respond to requests under this Section L within a reasonable period after the request is made; and
- b.* must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information.

End of section L
**“Correction of
personal information”**

Miscellaneous



31. Policy breaches

- 31.1** 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).
- 31.2** Staff are trained internally on compliance and their regulatory obligation to DVM. They are encouraged to respond appropriately to, and report all breaches of the law and other incidents of non-compliance, including DVM' policies, and seek guidance if they are unsure.
- 31.3** Staff must report breaches of this Policy directly to the Compliance Officer.

32. Retention of forms

- 32.1** The Compliance Officer will retain the completed forms for seven (7) years in accordance with DVM' Document Retention Policy. The completed forms are retained for future reference and review.

32.2 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 DVM' compliance obligations, but as a way of minimising risk.

Issued by DV Markets
“4 June 2019”