Privacy Policy

Omnium (NSW) Pty Ltd

Company:	Omnium (NSW) Pty Ltd
ABN:	45 101 181 015
AFSL:	500823
Date Updated:	01/11/18

TABLE OF CONTENTS

VERSION CONTROL 4

SECTION A – INTRODUCTION 5

1. INTRODUCTION 5

2. WHEN DOES THIS POLICY APPLY? 5

3. GLOSSARY 5

SECTION B – CONSIDERATION OF PERSONAL INFORMATION PRIVACY 6

4. PRIVACY STATEMENT 6

SECTION C – COLLECTION OF PERSONAL INFORMATION (SOLICITED PERSONAL INFORMATION) 7

5. PERSONAL INFORMATION (OTHER THAN SENSITIVE INFORMATION) 7

6. SENSITIVE INFORMATION 7

7. MEANS OF COLLECTION 7

8. INFORMATION COLLECTED BY OMNIUM 8

9. PURPOSE OF COLLECTION 8

SECTION D – COLLECTION OF PERSONAL INFORMATION (UNSOLICITED PERSONAL INFORMATION) 8

10. DEALING WITH UNSOLICITED PERSONAL INFORMATION 9

SECTION E – NOTIFICATION OF THE COLLECTION OF PERSONAL INFORMATION 9

11. NOTIFICATION OF COLLECTION 9

SECTION F – USE OR DISCLOSURE OF PERSONAL INFORMATION 10

12. USE OR DISCLOSURE 10

13. WHO DOES OMNIUM DISLCOSE PERSONAL INFORMATION TO? 10

SECTION G – DIRECT MARKETING 11

14. DIRECT MARKETING 11

15. EXCEPTION – PERSONAL INFORMATION OTHER THAN SENSITIVE INFORMATION 11

16. EXCEPTION – SENSITIVE INFORMATION 12

17. REQUESTS TO STOP DIRECT MARKETING 12

SECTION H – CROSS BORDER DISCLOSURE OF PERSONAL INFORMATION 12

18. DISCLOSING PERSONAL INFORMATION TO CROSS BORDER RECIPIENTS 12

SECTION I – ADOPTION, USE OR DISCLOSURE OF GOVERNMENT IDENTIFIERS 13

19. ADOPTION OF GOVERNMENT RELATED IDENTIFIERS 13

20. USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS 13

SECTION J – INTEGRITY OF PERSONAL INFORMATION 14

21. QUALITY OF PERSONAL INFORMATION 14

22. SECURITY OF PERSONAL INFORMATION 14

23. STORAGE OF PERSONAL INFORMATION 14

SECTION K – ACCESS TO, AND CORRECTION OF, PESRONAL INFORMATION 14

24. ACCESS 14

25. EXCEPTIONS 15

26. REFUSAL TO GIVE ACCESS 15

SECTION L – CORRECTION OF PERSONAL INFORMATION 16

27. CORRECTION OF INFORMATION 16

28. REFUSAL TO CORRECT INFORMATION 16

29. REQUEST FROM A CLIENT TO ASSOCIATE A STATEMENT WITH THEIR INFORMATION 16

30. DEALING WITH REQUESTS 16

SECTION M – MISCELLANEOUS 17

31. POLICY BREACHES 17

32. RETENTION OF FORMS 17

VERSION CONTROL

Version Number	Date Updated	Notes
1	03/03/2017	Original document prepared and finalised.
1.1	01/11/2018	Updated to reflect AFCA change

SECTION A – INTRODUCTION

1. INTRODUCTION

1.1 As part of Omnium (NSW) Pty Ltd (**"Omnium"**) process to ensure that it continues to maintain the highest levels of professional integrity and ethical conduct, Omnium 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 Omnium in complying with the requirements of the *Privacy Act 1988* (Cth) and the Australian Privacy Principles in protecting the personal information Omnium holds about its clients.

2. WHEN DOES THIS POLICY APPLY?

2.1 This Policy applies to all representatives and employees of Omnium 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 1988.
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	Omnium collects personal information only if Omnium 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	Omnium *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 1988
Permitted health situation	As defined in s16B of the Privacy Act 1988
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: (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) 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.

SECTION B – CONSIDERATION OF PERSONAL INFORMATION PRIVACY

4. PRIVACY STATEMENT

4.1 Omnium's Compliance Officer must ensure that at all times the provisions of this policy are implemented in the day to day running of Omnium.

4.2 The Compliance Officer must ensure that at all times this Policy:

(a) is current and reflects the latest applicable Australian laws; and

(b) contains the following information:

(i) the kinds of personal information that Omnium collects and holds;

(ii) how Omnium collects and holds personal information;

(iii) the purposes for which Omnium collects, holds, uses and discloses personal information;

(iv) how an individual may complain about a breach of the Australian Privacy Principles, or other relevant legislation that binds Omnium, and how Omnium will deal with such a complaint;

(v) whether Omnium is likely to disclose personal information to overseas recipients;

(vi) if Omnium 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 Omnium must ensure that the Omnium's Privacy Statement is available free of charge and in such form as appropriate. Omnium will make the Privacy Statement available on its website.

4.4 If the Privacy Statement is requested in a particular form, Omnium 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 Omnium.

5.2 Omnium must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of Omnium's functions or activities.

5.3 Omnium's functions or activities include:

(a) Research on Life Insurance policies

(b) Quoting software for Life Insurance premiums for financial advisers

(c) Quote and apply software for Life insurers

(d) Other data and analytical tools for the life insurance industry

*(e) Omnium "**does not retail or wholesale"** life insurance products nor does it give any financial advice of any nature.*

6. SENSITIVE INFORMATION

6.1 Omnium 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 Omnium'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 Omnium; or

(d) a permitted health situation exists in relation to the collection of the information by Omnium.

7. MEANS OF COLLECTION

7.1 Omnium must only collect personal information by lawful and fair means.

7.2 Omnium 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 Omnium to liaise with someone else.

7.3 Omnium will collect or pass on personal information from an individual when:

(a) A client or financial adviser uses the software that Omnium has built and hosts to submit a Life insurance Application Form.

(b) a Client provides the information to Omnium's representatives over the telephone or via email;

(c) a Client provides the information to Omnium on the website;

8. INFORMATION COLLECTED BY Omnium

8.1 The information Omnium collects may include the following:

(a) name;

(b) date of birth;

(c) postal or email address; or

(d) phone numbers;

(e) other information Omnium 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 Omnium, the individual's personal information will be collected and held for the purposes of:

(a) checking whether an individual is eligible for Omnium's product or service;

(b) providing the individual with Omnium's product or service;

(c) managing and administering Omnium's product or service;

(d) protecting against fraud, crime or other activity which may cause harm in relation to Omnium's products or services;

(e) complying with legislative and regulatory requirements in any jurisdiction;

(f) to assist Omnium in the running of its business;

(g) As part of the process of applying for life insurance via one of Omnium's quote and apply solutions that an insurer has engaged Omnium to build.

9.2 Omnium 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.

SECTION D – COLLECTION OF PERSONAL INFORMATION (UNSOLICITED PERSONAL INFORMATION)

10. DEALING WITH UNSOLICITED PERSONAL INFORMATION

10.1 If Omnium:

(a) receives personal information about an individual; and

(b) the information is not solicited by Omnium

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

10.3 If Omnium:

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

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

Omnium 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 Omnium must notify the individual of the following matters in the Privacy Statement:

(a) Omnium's identity and contact details;

(b) if Omnium collects the personal information from a third party or the individual is not aware that Omnium has collected the personal information, the fact that Omnium 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 Omnium collects the personal information;

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

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

(g) that Omnium'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 Omnium and seek correction of such information;

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

(i) whether Omnium will disclose the personal information to overseas recipients; and

(j) if Omnium discloses the personal information to overseas recipients – the 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.

SECTION F – USE OR DISCLOSURE OF PERSONAL INFORMATION

12. USE OR DISCLOSURE

12.1 Where Omnium holds personal information about an individual that was collected for a particular purpose ("**the primary purpose**"), Omnium 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 Omnium to use or disclose the information for the secondary purpose and the secondary purpose is:

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

(ii) 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 Omnium; or

(e) Omnium 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 Omnium uses or discloses personal information in accordance with section 12.1(e), Omnium will keep 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 Omnium collects personal information from a related body corporate, this section 12 applies as if Omnium's primary purpose for the collection was the primary purpose for which the related body corporate collected the information.

13. WHO DOES Omnium DISLCOSE PERSONAL INFORMATION TO?

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

(a) organisations involved in maintaining, reviewing and developing Omnium's business systems, procedures and infrastructure, including testing or upgrading Omnium's computer systems;

(b) organisations involved in a corporate re-organisation;

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

(d) organisations involved in product planning and development;

(e) other organisations, who jointly with Omnium's, provide its products or services;

(f) authorised representatives who provide Omnium's products or services on its behalf;

(g) the individual's representatives, including your legal advisers;

(h) debt collectors;

(i) Omnium's financial advisers, legal advisers or auditors;

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

(k) external dispute resolution schemes;

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

SECTION G – DIRECT MARKETING

14. DIRECT MARKETING

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

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

(b) Omnium has collected the information from a third party; and either:

(i) Omnium has obtained the individual's consent to the use or disclose the information for the purpose of direct marketing; or

(ii) it is impracticable for Omnium to obtain the individual's consent; and

(c) in each direct marketing communication with the individual Omnium:

(i) includes a prominent statement that the individual may make such a request; or

(ii) 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 Omnium 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 Omnium uses or discloses personal information about an individual for the purposes of direct marketing by Omnium or facilitating direct marketing by another organisation, the individual may request:

(a) that Omnium no longer provide them with direct marketing communications;

(b) that Omnium does not use or disclose the individual's personal information for the purpose of facilitating direct marketing by another organisation;

(c) that Omnium provides the source of the personal information.

17.2 Where Omnium receives a request from an individual under section 17.1, Omnium 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 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 Omnium discloses personal information about an individual to a recipient who is not in Australia and who is not Omnium or the individual, Omnium must ensure that the overseas recipient does not breach the Australian Privacy Principles (with the exception of APP1).

18.2 The countries we may disclose an individual's personal information to include:

(a) None at this stage, Omnium does not anticipate engaging offshore marketing agencies at this point in time

18.3 Section 18.1 does not apply where:

(a) Omnium reasonably believes that:

(i) 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

(ii) 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:

(i) Omnium has informed the individual that if they consent to the disclosure of information Omnium will not take reasonable steps to ensure the overseas recipient does not breach the Australian Privacy Principles; and

(ii) 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) Privacy Act) exists in relation to the disclosure of the information by Omnium.

SECTION I – ADOPTION, USE OR DISCLOSURE OF GOVERNMENT IDENTIFIERS

19. ADOPTION OF GOVERNMENT RELATED IDENTIFIERS

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

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

(b) the identifier, Omnium 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, Omnium must ensure that such use or disclosure is:

(a) reasonably necessary for Omnium 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) 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, Omnium and the circumstances of the adoption are prescribed by regulations.

SECTION J – INTEGRITY OF PERSONAL INFORMATION

21. QUALITY OF PERSONAL INFORMATION

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

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

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

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

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

23. STORAGE OF PERSONAL INFORMATION

23.1 Omnium stores personal information in different ways, including:

(a) electronically secure data centres which are located in Australia and owned by either Omnium or external service providers; or onsite on Omnium servers

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

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

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

(iii) all employees are required to complete training about information security;

(iv) Omnium regularly monitors and reviews its compliance with internal policies and industry best practice;

SECTION K – ACCESS TO, AND CORRECTION OF, PESRONAL INFORMATION

24. ACCESS

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

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

24.3 Omnium 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 Omnium and the individual.

24.4 Omnium 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 Omnium is not required to give an individual access to their personal information if:

(a) Omnium 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 if frivolous or vexatious; or

(d) the information relates to existing or anticipated legal proceedings between Omnium and the individual, and would not be accessible by the process of discovery in those proceedings; or

(e) giving access would reveal intentions of Omnium 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) Omnium 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 Omnium in connection with a commercially sensitive decision-making process.

26. REFUSAL TO GIVE ACCESS

26.1 If Omnium refuses to give access in accordance with section 24 or to give access in the manner requested by the individual, Omnium 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 Omnium refuses to give access under section 25.1(j) Omnium 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 Omnium must take reasonable steps to correct all personal information, having regard to the purpose for which the information is held where:

(a) Omnium is satisfied the information is inaccurate, out of date, incomplete, irrelevant or misleading; or

(b) the individual requests Omnium corrects the information.

27.2 Where Omnium corrects personal information about an individual that Omnium previously disclosed to another APP entity and the individual requests Omnium to notify the other APP entity of the correction, Omnium 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 Omnium refuses to correct personal information as requested by the individual, Omnium 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) Omnium refuses to correct personal information as requested by the individual; and

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

Omnium 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 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 Omnium 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.

SECTION M – 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 1988 (Cth)).

31.2 Staff are trained internally on compliance and their regulatory obligation to Omnium. They are encouraged to respond appropriately to, and report all breaches of the law and other incidents of non-compliance, including Omnium's 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 Omnium's 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 Omnium's compliance obligations, but as a way of minimising risk.

Issued by Omnium (NSW) Pty Ltd

01/11/2018