GDPR DATA PROTECTION POLICY

COMSEC INVESTIGATIONS LTD

123 ALDERSGATE STREET
LONDON
EC1A 4JQ

Important information

In line with Article 24 GDPR (EU) 2016/679, taking into account the nature, scope, context and purposes of processing as well as the risks to the rights and freedoms of natural persons, Comsec Investigations Ltd ("the Company") has implemented appropriate technical and organisational measures to ensure pursuance to the General Data Protection Regulation (GDPR). This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

Review date: 31st August 2020

Next review date: 31st August 2021

Comsec, 123 Aldersgate Street, London EC1A 4JQ | t +44 (0)207 553 7960 | f +44 (0)207 553 7970 | e info@comsechq.com

General Data Protection Regulation (GDPR)

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy.

In line with Article 5 of the GDPR, the Company must apply the following principles:-

1. Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
2. Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
4. Accuracy	Personal data shall be accurate and, where necessary, kept up to date.
5. Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
6. Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
7. Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR.

1. Scope

1.1 The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all

Comsec, 123 Aldersgate Street, London EC1A 4JQ | t +44 (0)207 553 7960 | f +44 (0)207 553 7970 | e info@comsechq.com

individuals with whom it deals.

1.2 The Company's Data Protection Officer is **Anya Worboys**. The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

1.3 All managers and heads of departments are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of the Company comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.

1.4 Any questions relating to this Policy or to Data Protection Law should be referred to the Data Protection Officer. In particular, the Data Protection Officer should always be consulted in the following cases:

a) if there is any uncertainty relating to the lawful basis on which personal data is to be collected, held, and/or processed;

b) if consent is being relied upon in order to collect, hold, and/or process personal data;

c) if there is any uncertainty relating to the retention period for any particular type(s) of personal data;

d) if any new or amended privacy notices or similar privacy-related documentation are required;

e) if any assistance is required in dealing with the exercise of a data subject's rights (including, but not limited to, the handling of subject access requests);

f) if a personal data breach (suspected or actual) has occurred;

g) if there is any uncertainty relating to security measures (whether technical or organisational) required to protect personal data;

h) if personal data is to be shared with third parties (whether such third parties are acting as data controllers or data processors);

i) if personal data is to be transferred outside of the EEA and there are questions relating to the legal basis on which to do so;

j) when any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities, which will require a Data Protection Impact Assessment;

k) when personal data is to be used for purposes different to those for which it was originally collected;

l) if any automated processing, including profiling or automated decision-making, is to be carried out; or

m) if any assistance is required in complying with the law applicable to direct marketing.

Comsec, 123 Aldersgate Street, London EC1A 4JQ | t +44 (0)207 553 7960 | f +44 (0)207 553 7970 | e info@comsechq.com

2. **The Rights of Data Subjects**

The GDPR sets out the following key rights applicable to data subjects:

2.1 The right to be informed;

2.2 the right of access;

2.3 the right to rectification;

2.4 the right to erasure (also known as the 'right to be forgotten');

2.5 the right to restrict processing;

2.6 the right to data portability;

2.7 the right to object; and

2.8 rights with respect to automated decision-making and profiling.

3. **Lawful, Fair, and Transparent Data Processing**

3.1 Data Protection Law seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, the GDPR states that processing of personal data shall be lawful if at least one of the following applies:

a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

b) the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;

c) the processing is necessary for compliance with a legal obligation to which the data controller is subject;

d) the processing is necessary to protect the vital interests of the data subject or of another natural person;

e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

f) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4. **Consent**

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, the following shall apply:

4.1 Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.

Comsec, 123 Aldersgate Street, London EC1A 4JQ | t +44 (0)207 553 7960 | f +44 (0)207 553 7970 | e info@comsechq.com

4.2 Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters.

4.3 Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.

4.4 If personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.

4.5 In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to ensure that the Company can demonstrate its compliance with consent requirements.

5. Specified, Explicit, and Legitimate Purposes

5.1 The Company collects and processes the personal data set out in Clause 19 of this Policy. This includes:

a) personal data collected directly from data subjects**;** and

b) personal data obtained from third parties.

5.2 The Company only collects, processes, and holds personal data for the specific purposes set out in Clause 19 of this Policy (or for other purposes expressly permitted by the GDPR).

5.3 Data subjects must be kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Clause 12 for further information on keeping data subjects informed.

6. Adequate, Relevant, and Limited Data Processing

6.1 The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Clause 5 above, and as set out in Clause 19, below.

6.2 Employees, agents, contractors, or other parties working on behalf of the Company may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected.

6.3 Employees, agents, contractors, or other parties working on behalf of the Company may process personal data only when the performance of their job duties requires it. Personal data held by the Company cannot be processed for any unrelated reasons.

Comsec, 123 Aldersgate Street, London EC1A 4JQ | t +44 (0)207 553 7960 | f +44 (0)207 553 7970 | e info@comsechq.com

7. Accuracy of Data and Keeping Data Up-to-Date

7.1 The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Clause 17, below.

7.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. Data Retention

8.1 The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

8.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

8.3 For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

9. Secure Processing

9.1 The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

9.2 All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data.

9.3 Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all personal data as follows:

a) only those with a genuine need to access and use personal data and who are authorised to do so may access and use it;

b) personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and

c) authorised users must always be able to access the personal data as required for the authorised purpose or purposes.

10. Accountability and Record-Keeping

10.1 The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.

10.2 The Company shall follow a privacy by design approach at all times when collecting, holding, and processing personal data. Data Protection Impact Assessments shall be conducted if any processing presents a significant risk

Comsec, 123 Aldersgate Street, London EC1A 4JQ | t +44 (0)207 553 7960 | f +44 (0)207 553 7970 | e info@comsechq.com

to the rights and freedoms of data subjects (please refer to Clause 14 for further information).

10.3 All employees, agents, contractors, or other parties working on behalf of the Company shall be given appropriate training in data protection and privacy, addressing the relevant aspects of Data Protection Law, this Policy, and all other applicable Company policies.

10.4 The Company's data protection compliance shall be regularly reviewed and evaluated by means of Data Protection Audits.

10.5 The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

10.5.1 the name and details of the Company, its Data Protection Officer, and any applicable third-party data transfers (including data processors and other data controllers with whom personal data is shared);

10.5.2 the purposes for which the Company collects, holds, and processes personal data;

10.5.3 the Company's legal basis or bases (including, but not limited to, consent, the mechanism(s) for obtaining such consent, and records of such consent) for collecting, holding, and processing personal data;

10.5.4 details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;

10.5.5 details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

10.5.6 details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy);

10.5.7 details of personal data storage, including location(s);

10.5.8 detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

11. Data Protection Impact Assessments and Privacy by Design

11.1 In accordance with the privacy by design principles, the Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects.

11.2 The principles of privacy by design should be followed at all times when collecting, holding, and processing personal data. The following factors should be taken into consideration:

a) the nature, scope, context, and purpose or purposes of the collection, holding, and processing;

b) the state of the art of all relevant technical and organisational measures to be taken;

c) the cost of implementing such measures; and

Comsec, 123 Aldersgate Street, London EC1A 4JQ | t +44 (0)207 553 7960 | f +44 (0)207 553 7970 | e info@comsechq.com

d) the risks posed to data subjects and to the Company, including their likelihood and severity.

11.3 Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

a) the type(s) of personal data that will be collected, held, and processed;

b) the purpose(s) for which personal data is to be used;

c) the Company's objectives;

d) how personal data is to be used;

e) the parties (internal and/or external) who are to be consulted;

f) the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;

g) risks posed to data subjects;

h) risks posed both within and to the Company; and

i) proposed measures to minimise and handle identified risks.

12. Keeping Data Subjects Informed

12.1 The Company shall provide the information set out in Clause 12.2 to every data subject:

a) where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

b) where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

i) if the personal data is used to communicate with the data subject, when the first communication is made; or

ii) if the personal data is to be transferred to another party, before that transfer is made; or

iii) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

12.2 The following information shall be provided in the form of a privacy notice:

a) details of the Company including, but not limited to, contact details, and the names and contact details of any applicable representatives and its Data Protection Officer;

b) the purpose(s) for which the personal data is being collected and will be processed (as detailed in Clause 19 of this Policy) and the lawful basis justifying that collection and processing;

c) where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;

d) where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

e) where the personal data is to be transferred to one or more third parties, details of those parties;

Comsec, 123 Aldersgate Street, London EC1A 4JQ | t +44 (0)207 553 7960 | f +44 (0)207 553 7970 | e info@comsechq.com

f) where the personal data is to be transferred to a third party that is located outside of the EEA, details of that transfer, including but not limited to the safeguards in place (see Clause 26 of this Policy for further details);

g) details of applicable data retention periods;

h) details of the data subject's rights under the GDPR;

i) details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;

j) details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);

k) where the personal data is not obtained directly from the data subject, details about the source of that personal data;

l) where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

m) details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

13. Data Subject Access

13.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.

13.2 Employees wishing to make a SAR should do using a Subject Access Request Form, sending the form to the Company's Data Protection Officer at the address below.

13.3 Responses to SARs must normally be made within one month of receipt, however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

13.4 All SARs received shall be handled by the Company's Data Protection Officer.

13.5 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. Rectification of Personal Data

14.1 Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

Comsec, 123 Aldersgate Street, London EC1A 4JQ | t +44 (0)207 553 7960 | f +44 (0)207 553 7970 | e info@comsechq.com

14.2 The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

14.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

15. Erasure of Personal Data

15.1 Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

a) it is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

b) the data subject wishes to withdraw their consent to the Company holding and processing their personal data;

c) the data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Clause 17 of this Policy for further details concerning the right to object);

d) the personal data has been processed unlawfully;

e) the personal data needs to be erased in order for the Company to comply with a particular legal obligation**;**

15.2 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

15.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. Restriction of Personal Data Processing

16.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

16.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

Comsec, 123 Aldersgate Street, London EC1A 4JQ | t +44 (0)207 553 7960 | f +44 (0)207 553 7970 | e info@comsechq.com

17. **Objections to Personal Data Processing**

17.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests, for direct marketing (including profiling).

17.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

17.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing promptly.

18. **Profiling**

18.1 The Company uses personal data for profiling purposes only in the exceptional case where a third party client has requested it. Such profiling activities will be generic in nature; by way of example, the personal data may be profiled to identify the number of data subjects residing in a particular geographical area.

18.2 The activities described in this Clause 18 are generally prohibited under Data Protection Law where the resulting decisions have a legal or similarly significant effect on data subjects unless one of the following applies:

a) the data subject has given their explicit consent;

b) the processing is authorised by law; or

c) the processing is necessary for the entry into, or performance of, a contract between the Company and the data subject.

18.3 If special category personal data is to be processed in this manner, such processing can only be carried out if one of the following applies:

a) the data subject has given their explicit consent; or

b) the processing is necessary for reasons of substantial public interest.

18.4 Where decisions are to be based solely on automated processing (including profiling), data subjects have the right to object, to challenge such decisions, request human intervention, to express their own point of view, and to obtain an explanation of the decision from the Company. Data subjects must be explicitly informed of this right at the first point of contact.

18.5 In addition to the above, clear information must be provided to data subjects explaining the logic involved in the decision-making or profiling, and the significance and envisaged consequences of the decision or decisions.

18.6 When personal data is used for any form of automated processing, automated decision-making, or profiling, the following shall apply:

a) appropriate mathematical or statistical procedures shall be used;

b) technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and

Comsec, 123 Aldersgate Street, London EC1A 4JQ | t +44 (0)207 553 7960 | f +44 (0)207 553 7970 | e info@comsechq.com

c) all personal data to be processed in this manner shall be secured in order to prevent discriminatory effects arising (see Clauses 19 to 24 of this Policy for more details on data security and organisational measures).

19. **Personal Data Collected, Held, and Processed**

The following personal data is collected, held, and processed by the Company:

Type of Data	Purpose of Data
Addresses	The prevention of crime and intellectual property infringement
Postcodes	The prevention of crime and intellectual property infringement
Name details or names as profiled on websites	The prevention of crime and intellectual property infringement
Images of auctions	The prevention of crime and intellectual property infringement
Phone numbers where advertised	The prevention of crime and intellectual property infringement
Email addresses	The prevention of crime and intellectual property infringement
IP addresses	The prevention of crime and intellectual property infringement
Images of social media posts	The prevention of crime and intellectual property infringement

20. **Data Security - Transferring Personal Data and Communications**

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

20.1 All emails containing personal data must be encrypted;

20.2 All emails containing personal data must be marked “confidential;”

20.3 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

20.4 Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

20.5 Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;

20.6 Where personal data is to be transferred in hardcopy form it should be passed

Comsec, 123 Aldersgate Street, London EC1A 4JQ | t +44 (0)207 553 7960 | f +44 (0)207 553 7970 | e info@comsechq.com

directly to the recipient;

20.7 All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential."

21. Data Security - Storage

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

21.1 All electronic copies of personal data should be stored securely using passwords and data encryption;

21.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

21.3 All personal data stored electronically should be backed up daily.

21.4 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise without the formal written approval of Benjamin Fourmond and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;

21.5 No personal data should be transferred to any device personally belonging to an employee, agent, contractor, or other party working on behalf of the Company and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

22. Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Company's Data Retention Policy.

23. Data Security - Use of Personal Data

The Company shall ensure that the following measures are taken with respect to the use of personal data:

23.1 No personal data may be shared informally and if an employee, agent, contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from Benjamin Fourmond;

23.2 No personal data may be transferred to any employee, agent, contractor, or other party, whether such parties are working on behalf of the Company or not, without the authorisation of Benjamin Fourmond;

Comsec, 123 Aldersgate Street, London EC1A 4JQ | t +44 (0)207 553 7960 | f +44 (0)207 553 7970 | e info@comsechq.com

23.3 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, contractors, or other parties at any time;

23.4 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.

24. Data Security - IT Security

The Company shall ensure that the following measures are taken with respect to IT and information security:

24.1 All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols;

24.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

24.3 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible;

24.4 No software may be installed on any Company-owned computer or device without the prior approval of the Benjamin Fourmond.

25. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

25.1 All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under Data Protection Law and under this Policy, and shall be provided with a copy of this Policy;

25.2 Only employees, agents, contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;

25.3 All sharing of personal data shall comply with the information provided to the relevant data subjects and, if required, the consent of such data subjects shall be obtained prior to the sharing of their personal data;

25.4 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

25.5 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;

Comsec, 123 Aldersgate Street, London EC1A 4JQ | t +44 (0)207 553 7960 | f +44 (0)207 553 7970 | e info@comsechq.com

25.6 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

25.7 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

25.8 All personal data held by the Company shall be reviewed periodically;

25.9 The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

25.10 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of Data Protection Law and this Policy;

25.11 All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and Data Protection Law;

25.12 Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

26. Transferring Personal Data to a Country Outside the EEA

26.1 The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

26.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

26.2.1 the transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

26.2.2 the transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

26.2.3 the transfer is made with the informed and explicit consent of the relevant data subject(s);

Comsec, 123 Aldersgate Street, London EC1A 4JQ | t +44 (0)207 553 7960 | f +44 (0)207 553 7970 | e info@comsechq.com

26.2.4 the transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);

26.2.5 the transfer is necessary for important public interest reasons;

26.2.6 the transfer is necessary for the conduct of legal claims;

26.2.7 the transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

26.2.8 the transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

27. Data Breach Notification

27.1 All personal data breaches must be reported immediately to the Company's Data Protection Officer.

27.2 If an employee, agent, contractor, or other party working on behalf of the Company becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question should be carefully retained.

27.3 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

27.4 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Clause 27.3) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

27.5 Data breach notifications shall include the following information:

27.5.1 The categories and approximate number of data subjects concerned;

27.5.2 The categories and approximate number of personal data records concerned;

27.5.3 The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);

27.5.4 The likely consequences of the breach;

27.5.5 Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Comsec, 123 Aldersgate Street, London EC1A 4JQ | t +44 (0)207 553 7960 | f +44 (0)207 553 7970 | e info@comsechq.com

Complaints handling

Upon receipt of a data subject complaint the Company will internally investigate the issue. The Company will inform the data subject of progress and eventually the outcome of the complaint. This must be communicated within a reasonable period.

Where the issue cannot be resolved between the data subject and the Company, they may choose to seek redress through mediation, litigation or via complaint to the ICO. The Company must inform data subjects of their right to complain directly to the ICO.

In order to exercise all rights, queries and complaints please contact:

Anya Worboys
Comsec Investigations – Data Protection & GDPR Compliance Department
123 Aldersgate Street
London
EC1A 4JQ
info@comsechq.com
020 75537960

Appendix 1

Personal data	Any information (including opinions and intentions) which relates to an identified or identifiable natural person
Data controller	A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
Data subject	The identified or identifiable natural person to which the data refers
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her
International organisation	An organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.
ICO	Data protection supervisory authority: Information Commissioner's Office Telephone: 03031-231-113 Opening hours: Monday to Friday 9am- 5pm

Comsec, 123 Aldersgate Street, London EC1A 4JQ | t +44 (0)207 553 7960 | f +44 (0)207 553 7970 | e info@comsechq.com