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 have implemented appropriate technical and organisational measures to ensure pursuance to the General Data Protection Regulation (GDPR). This policy stands as the cornerstone to Comsec's compliance with the GDPR and is reviewed and updated accordingly.

Review date: 27 March 2018

Board approval: 09 May 2018

Next review date: 22 April 2019

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, Comsec must conform to the following principles at all times:-

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.

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

Comsec is at all times responsible for, and able to demonstrate compliance with the aforementioned principles.

Compliance monitoring

In order to maintain a high level of compliance in relation to the rules stipulated within this policy, Comsec carries out an annual Data Protection compliance audit. Conducting a through diagnostic audit allows Comsec to recognise any deficiencies or areas for improvement; upon mitigation, ensuring total compliance to the GDPR. Examples of the areas covered within an audit include:

(a) Data protection governance, and the structures, policies and procedures to ensure GDPR compliance
(b) The processes for managing both electronic and manual records containing personal data
(c) The processes responding to any request for personal data
(d) The technical and organisational measures in place to ensure that there is adequate security over personal data
(e) The provision and monitoring of staff data protection training and the awareness of data protection
(f) Data audit as per Appendix 2 (below)

Data subject rights and requests

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Comsec have in place adequate systems and controls to enable and facilitate the application of the eight data subject rights listed above.

When a data subject makes a request, Comsec will embark on a pragmatic decision-making process headed up by Victoria Horsgood (HR & GDPR Compliance Department).

Unless Comsec deem requests to be excessive or unnecessary in their nature, no fee will be charged to the data subjects for considering and/or complying with requests.

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

Rights to access

All requests of this nature should be referred to the Compliance Department. Comsec will respond to requests within 30 days.

The data subject has the right to obtain the following information from Comsec:

(a) The purposes of the processing
(b) The categories of personal data concerned
(c) The recipients or categories personal data stored for the data subject
(d) The envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
(e) The use of any automated decision-making e.g. profiling

When requested, Comsec shall provide a copy of the personal data held. For any further copies requested by the data subject, Comsec may charge a reasonable fee based on administrative costs. Where requests are made via electronic means, Comsec shall provide the data in a commonly used electronic form.

Right to rectification

Comsec will ensure all data subjects are able to exercise their right to obtain from the firm, without undue delay, the rectification of inaccurate personal data concerning him or her.

Right to erasure

Without undue delay Comsec will erase personal data of a data subject where requested, and where one of the following grounds applies.

(a) The personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
(b) The data subject withdraws consent which the processing is based on, and where there is no other legal ground for the processing
(c) The data subject objects to the processing and there are no overriding legitimate grounds for the processing, or where the data subject objects to processing
(d) The personal data has been unlawfully processed
(e) The personal data has to be erased compliant with a legal obligation in the member state law
(f) The personal data have been collected in relation to the offer of information society services

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

Article 17 3 (b) GDPR, states that the right to erasure is disapplied where the firm must retain data in order to comply with other applicable regulation. The superseding regulations in Comsec's case are, The Money Laundering Regulations requirement for firms to hold KYC data for 5 years, and MiFID II Article 16 requirements on record keeping. This is referred to in Comsec's privacy notice.

Right to restrict processing

Comsec will cease processing of personal data in the following circumstances:

(a) Where an individual contests the accuracy of the personal data, Comsec will restrict the processing until the accuracy of the data is verified
(b) Where an individual has objected to the processing and the firm are considering whether we have legitimate grounds to override those of the individual
(c) When processing is found to be unlawful and the individual opposes erasure and requests a restriction instead
(d) If we no longer need the data but the individual requires the data to establish, exercise of defend a legal claim

Right to data portability

The right to portability only applies:

(a) To personal data an individual has provided to a controller
(b) Where the processing is based on the individual's consent or for the performance of a contract
(c) When processing is carried out by automated means

To comply, Comsec must:

(a) Provide the personal data in a structured, commonly used and machine readable format.
(b) Provide the data free of charge (unless excessive or unnecessary)
(c) If requested and technically feasible, transmit the data directly to another organisation.
(d) Consider possible prejudice of the rights of individuals, where the personal data concerns more than one individual

Consent

Consent must be given by a clear affirmative act, which establishes freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of their data. Comsec will obtain consent via a written statement, by electronic means, or an oral statement.

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

Comsec request, manage and record consent pursuant to Articles 5, 6, 7 and 9 of GDPR.

(a) Comsec check that consent is the most appropriate lawful basis for processing
(b) Comsec make the request for consent prominent and separate from our terms and conditions
(c) Comsec request a positive opt in
(d) Comsec do not use pre-ticked boxes or any other type of default consent
(e) Comsec use clear, plain language that is easy to understand
(f) Comsec specify why we want the data and its purpose
(g) Comsec provide granular options to consent separately to different purposes and types of processing
(h) Comsec name our organisation and any third party controllers who will be relying on our consent
(i) Comsec ensure that individuals can refuse to consent without detriment
(j) Avoid making consent a precondition of service

Comsec record when and how the firm obtained consent from individuals. The firm also keep a record of the exact information originally provided.

Exercises Comsec may carry out to ensure the appropriate management of consent include the following.

(a) Comsec regularly review consents to check that the relationship, the processing and the purposes have not changed
(b) Comsec have processes in place to refresh consent at appropriate intervals, including any parental consents
(c) Comsec consider using privacy dashboards or other preference-management tools as a matter of good practice
(d) Comsec make it easy for individuals to withdraw their consent at any time, and publicise how this is done
(e) Comsec act on withdrawals of consent as soon as possible
(f) Comsec do not penalise individuals who wish to withdraw consent

Comsec will not infer consent from silence or inactivity. When the processing of personal data has multiple purposes, Comsec will obtain consent for all of them. Where a data subject's consent is to be given following a request by electronic means, Comsec will ensure the request is clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

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

Data privacy by design

Comsec have in place technical and organisational measures which integrate data protection into processing activities.

Privacy and data protection is a key consideration in the early stages of any project Comsec undertakes
For example, when:

(a) Building new IT systems for storing or accessing personal data
(b) Developing legislation, policy or strategies that have privacy implications
(c) Embarking on a data sharing initiative
(d) Using data for new purposes

Privacy and data protection considerations will be integrated into Comsec's risk management methodologies and policies.

Data protection impact assessments (DPIA)
Comsec will carry out a DPIA where data processing is likely to result in high risk to individuals, for example:

(a) Where a new technology is being implemented
(b) Where a profiling operation is likely to significantly affect individuals
(c) Where there is large scale processing of special categories of data

In assessing the level of risk Comsec will consider both the likelihood and severity of any impact to individuals concerned.

Comsec ensure that there is a sound understanding of DPIA amongst certain members of the firm.

(a) Comsec provide training so that all staff understand the need to consider a DPIA at the early stages of any plan involving personal data
(b) Comsec's existing policies, processes and procedures include references to DPIA requirements, where applicable
(c) Comsec understand the types of processing that requires a DPIA
(d) Comsec will create and document a robust DPIA process
(e) Comsec will provide training for relevant staff on how to carry out a DPIA

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

Breach Reporting

In the case of a personal data breach, Comsec shall without undue delay, and where practicable, notify the ICO not later than 72 hours after having become aware of the breach. This is not required, where the breach will not likely result in a risk to the rights and freedoms of natural persons. Where the notification is not made with 72 hours Comsec must provide a valid reason for the delay. ICO contact details can be found in Appendix 1.

Notifications made by Comsec shall at least:

(a) Describe the nature of the personal data breach
(b) Communicate the name and contact details of the relevant department handling the data breach.
(c) Describe the likely consequences of the personal data breach
(d) Describe the measure taken or proposed to be taken by Comsec to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

Where the personal data breach is likely to result in a high risk to the rights and freedoms of subjects, Comsec shall communicate the data breach to the data subject without undue delay.

Comsec shall communicate the matter to the data subject in clear and plain language the nature of the personal data breach, detailing at least the information in points (b), (c) and (d) as above.

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

Record keeping

Comsec employ fewer than 250 people, and so, Article 30 GDPR is technically not applicable. That being said, due to the other data monitoring requirements dictated by GDPR and for best practice, Comsec will maintain a record of processing activities under its responsibility. That record shall contain the following information:

The name and contact details of the controller

(a) The purposes of the processing
(b) A description of the categories of data subjects and of the categories of personal data
(c) The recipients to whom the personal data has been or will be disclosed including recipients in third counties or international organisations
(d) Where applicable, transfers of personal data to a third country or international organisation, including the identification of that third country or international organisation
(e) Where possible, the envisaged time limits for erasure of the different categories of data
(f) Where possible, a description of the technical and organisation measures referred to in Article 32 (1)

Comsec keeps records in writing, and in electronic format.
If requested by the FCA/ICO, Comsec will make records available immediately.

Complaints handling

Upon receipt of a data subject complaint Comsec will internally investigate the issue. Comsec 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 Comsec, they may choose to seek redress through mediation, litigation procedure or via complaint to the ICO.
Comsec must inform data subjects of their right to complain directly to the ICO.
In order to exercise all rights, queries and complaints please contact:

Victoria Horsgood
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

Appendix 2.

Monitoring Data checklist

Details of the data held by Comsec	
Reason for holding that data	
Methods for obtaining that data	
Date that the data was obtained	
Individuals responsible for the data	
Data storage	
Data retention	
Data deletion methodology	

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