AerFin

Data Protection Policy

Revision 5: 14 July 2026

AerFin

Data protection policy

1. Purpose

The purpose of this Data Protection Policy (the "**Policy**") is to set out AerFin's (the "**Company**") approach to ensuring compliance with:

- the EU's General Data Protection Regulation ("**EU GDPR**");
- the UK's Data Protection Act 2018 ("**DPA 2018**") and the EU GDPR as implemented into English law by the UK European Union (Withdrawal) Act 2018 and updated by the Data (Use and Access) Act 2025 ("**UK GDPR**");
- Singapore's Personal Data Protection Act 2012 ("**PDPA**"); and
- U.S. state consumer privacy laws, including the Florida Digital Bill of Rights ("**FDBR**"), Fla. Stat. §§ 501.701–501.721, the Florida Information Protection Act ("**FIPA**"), Fla. Stat. § 501.171, the California Consumer Privacy Act ("**CCPA**") and any other U.S. state consumer privacy law that applies to the Company's Processing of Personal Data.

(collectively referred to as the "**Data Protection Laws**").

This Policy is structured to ensure compliance with the EU GDPR and UK GDPR / DPA 2018 as its baseline. As we also operate in Singapore and the U.S. which have their own data protection regulations, we have set out where we need to consider these which may supplement or deviate from the position taken under the baseline.

This Policy (and any other documents referred to herein), applies to all staff and associated entities of the Company, where such staff and entities deal with information and data which is subject to the Data Protection Laws (as more fully set out below) and sets out the basis upon which the Company will protect and Process any such data it collects.

Partners and other agencies or third parties who work with or for the Company and who have or may have access to or who may Process Personal Data will be expected to have read, understood and comply with this Policy. This Policy does not form part of any employee's contract of employment and may be amended at any time.

The Data Protection Officer, whose details are set out below, is responsible for ensuring compliance with the Data Protection Laws and with this Policy. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the Data Protection Officer or be reported in line with the Company's whistleblowing policy or grievance policy.

This Policy was last reviewed on 14 July 2026 (the "**Review Date**") and will be updated on or around the date that falls twelve (12) months from the Review Date.

Notwithstanding the foregoing, this Policy may be changed at any time as necessary, to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Laws.

2. Definitions

Capitalised terms used herein shall have the meanings set out below unless the context requires otherwise.

Consumer	For the purposes of applicable U.S. state

	privacy laws, means a natural person who is a resident of the relevant U.S. state acting in an individual or household context. An individual acting in a commercial or employment context is not a “Consumer.”
Data Controller	means the party who determines the purposes for which and the means by which Personal Data is Processed. For the purposes of the PDPA, references to "Data Controller" shall be construed as references to an "organisation" (as defined in the PDPA).
Data Processor	means the party who Processes Personal Data on behalf of the Data Controller. For the purposes of the PDPA, references to "Data Processor" shall be construed as references to a "data intermediary" (as defined in the PDPA).
DPC	means the Data Protection Commission, being the supervisory authority responsible for the administration and enforcement of the EU GDPR in Ireland.
EEA	means the European Economic Area.
Florida AG	means The Florida Attorney General, being the relevant supervisory authority responsible for enforcement of the FDBR and FIPA.
Personal Data	means data (whether stored electronically or paper based) relating to a living individual who can be identified directly or indirectly from that data (or from that data and other information in our possession).
Processing	means any activity that involves use of Personal Data, including without limitation, obtaining, recording or holding the data, organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal Data to third parties.
ICO	means the Information Commissioner’s Office or the Information Commissioner, being the supervisory authority responsible for the administration and enforcement of the DPA 2018 and UK GDPR.
PDPC	means the Personal Data Protection Commission of Singapore, being the supervisory authority responsible for the administration and enforcement of the PDPA.
Data Subject	means an identified or identifiable natural

	person who shares his or her Personal Data from whom Personal Data is Processed by the Company.
Special Categories of Personal Data	means: (i) under the UK and EU GDPR Personal Data about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric, physical or mental health condition, sexual orientation or sexual life. It can also include data about criminal offences or convictions; and/or (ii) Under the FDBR and other applicable U.S. state privacy laws: Personal Data revealing racial or ethnic origin; religious beliefs; mental or physical health diagnosis; sexual orientation; citizenship or immigration status; genetic or biometric data Processed for the purpose of uniquely identifying an individual; precise geolocation data (within approximately 1,800 feet); and Personal Data of a known child.

3. Scope of Data Protection Laws

The EU GDPR and UK GDPR / DPA 2018 apply to the Processing of Personal Data by all organisations established in the EU and UK. The EU and UK GDPR also applies to organisations outside of the EU / UK that offer goods or services to individuals in the EU / UK.

The PDPA applies to the collection, use and disclosure of Personal Data by the Company's Singapore branch. Therefore, the Company is subject to the Data Protection Laws and must Process any Personal Data in accordance with the provisions of this Policy.

U.S. state privacy laws, including the FDBR and FIPA, will apply to the Company insofar as it is Processing, collecting, and/or selling or sharing Personal Data in scope of those laws. For example, subject to the applicable thresholds, the FDBR applies to the Company's Processing of Personal Data of Florida residents acting in an individual or household context, and FIPA applies to the Company's handling of Personal Data of Florida residents.

Special Categories of Personal Data can only be Processed under strict conditions depending on the relevant jurisdiction, including with the consent of the individual unless an alternative lawful basis for Processing exists. For the avoidance of doubt, under the FDBR, the Company must obtain opt-in consent prior to Processing Sensitive Data of Florida Consumers.

4. Data Protection Principles

The Company is committed to ensuring that anyone Processing Personal Data on its behalf, must procure that such data is:

(a) Processed fairly, lawfully and in a transparent manner;

(b) Collected for specified, explicit and legitimate purposes and any further Processing is

completed for a compatible purpose;

(c) Adequate, relevant and limited to what is necessary for the intended purposes;

(d) Accurate, and where necessary, kept up to date;

(e) Kept in a form which permits identification for no longer than necessary for the intended purposes; and

(f) Processed in line with the individual's rights and 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.

5. Consent

Wherever possible, Personal Data should not be obtained, held, used or disclosed unless the individual has given consent. The Company understands 'consent' to mean that the Data Subject has been fully informed of the purpose of the intended Processing at the time of collection of the Personal Data and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. There should be some active communication between us and the individual such as signing a form (and the individual must sign the form freely of their own accord). This approach to consent also applies to the Company employees. However, the Company recognises that consent in an employment context is not always appropriate and we will rely on other lawful basis to Process employee Personal Data as appropriate. For example, under the UK and EU GDPR, consent is unlikely to be a valid lawful basis for employee Personal Data as it is difficult to prove that such consent is 'freely given' due to the power imbalance in an employer/employee relationship.

Under the UK, EU GDPR, and many U.S. state privacy laws, consent cannot be inferred from non-response to a communication. However, there are situations in certain jurisdictions we operate (e.g., Singapore) in which deemed consent provisions may apply, which will require case-by-case assessment at a local level.

For Special Categories of Personal Data, the Company's standard position is that explicit consent of Data Subjects must be obtained to comply with the Data Protection Laws unless an alternative lawful basis for Processing exists. For example, under the FDBR, the Company must obtain opt-in consent prior to Processing Sensitive Data of Florida Consumers. However, under the UK and EU GDPR or PDPA, the Company may determine that an alternative lawful basis for Processing this Personal Data is more appropriate.

When gathering Personal Data or establishing new data protection activities, the Company shall ensure that Data Subjects whose data is being Processed receive the relevant and appropriate data protection notices at the outset to inform them how their Personal Data will be used and, where appropriate, to obtain their consent.

In Singapore, where a Data Subject withdraws consent to the collection, use or disclosure of his or her Personal Data, the Company shall inform the Data Subject of the likely consequences of such withdrawal and shall cease (and cause its data intermediaries and agents to cease) the relevant Processing within a reasonable period of time.

6. Fair and Lawful Processing

The Data Protection Laws are intended to ensure that such Processing activities are done fairly and without adversely affecting the rights of the individual.

In the course of our business, the Company may collect and Process Personal Data of Data Subjects. This may include data we receive directly from a Data Subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, location data, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

The Company will only Process Personal Data in accordance with Data Protection Laws. Where it is acting as a Data Controller, it is required to have a lawful purpose in certain jurisdictions. Where it is acting as a Data Processor, it is not required to have a lawful purpose as it will be Processing Personal Data entirely on the instructions of another entity.

The lawful purpose the Company will rely on will depend on the circumstances of Processing and the applicable Data Protection Laws. For example:

- Under the UK and EU GDPR, the lawful purposes include (amongst others): whether the individual has given their consent, the Processing is necessary for performing a contract with the individual, for compliance with a legal obligation, or for the legitimate interest of the business (provided that such interest does not outweigh the rights and freedoms of the Data Subject). When Special Categories of Personal Data are being Processed, additional conditions must be met in accordance with Article 9 of the GDPR. The Company must also provide this information to individuals which it does through our Privacy Policy, available on our website.
- Under the PDPA, in certain circumstances the Company may determine that consent is deemed to have been given by a Data Subject, or that Personal Data may be collected, used or disclosed without the consent of the Data Subject where an applicable exception or exemption applies.

7. Notifying Individuals

If the Company collects Personal Data directly from an individual, the individual will be provided with our Privacy Policy, which will inform them about:

(a) The purpose or purposes for which the Company intends to Process that Personal Data, as well as the legal basis for the Processing;

(b) Where we rely upon the legitimate interests of the business to Process Personal Data, the legitimate interests pursued;

(c) The types of third parties, if any, with which the Company will share or disclose that Personal Data;

(d) The fact that the business intends to transfer Personal Data to a non-EEA country or international organisation (or, in respect of the Singapore branch, outside of Singapore) and the appropriate and suitable safeguards in place;

(e) How individuals can limit the Company's use and disclosure of their Personal Data.

(f) Information about the period that their information will be stored or the criteria used to determine that period;

(g) Their right to request from us, as the Data Controller, access to and rectification or erasure of Personal Data or restriction of Processing;

(h) Their right to object to Processing and their right to data portability;

(i) Their right to withdraw their consent at any time (if consent was given) without affecting the lawfulness of the Processing before the consent was withdrawn;

(j) Their right to complain to the Company if they believe we have infringed the DPA 2018 or UK GDPR (see Appendix 2 for further information for our complaints procedure);

(k) The right to lodge a complaint with the relevant supervisory authority;

(l) Other sources where Personal Data regarding the individual originated from and whether it came from publicly accessible sources;

(m) Whether the provision of the Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the Personal Data and any consequences of failure to provide the data;

(n) The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the individual.

(o) The Company will also inform Data Subjects whose Personal Data we Process that we are the Data Controller regarding that data.

In email and SMS marketing communications sent to US recipients, the Company will provide a method to unsubscribe from further marketing communications in accordance with applicable law. The Company will honour the Global Privacy Control (GPC) (https://globalprivacycontrol.org/) as a Universal Opt-Out Signal indicating a Consumer's preference to opt out of the sale of Personal Data and/or targeted advertising. The Company will not respond to web browser “do not track” signals. Please note that not all tracking will stop even if cookies are deleted. The Universal Opt-Out Signal is a signal communicated by a Consumer to indicate a preference to opt out of the sale of personal data and/or targeted advertising, including the GPC.

8. Adequate, Relevant and Non-excessive Processing

We will only collect Personal Data to the extent that it is required for the specific purpose notified to the Data Subject.

Personal Data obtained for one purpose should generally not be used for other unconnected purposes unless:

- The Data Subject has agreed to this or would otherwise reasonably expect the Personal Data to be used in this way; or
- We have conducted a compatibility assessment and determined that further purposes of Processing are compatible with the original collection purpose.

9. Accurate Data

The Company will ensure that the Personal Data held by it is accurate and kept up to date. The Company will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. The Company will take all reasonable steps to destroy or amend inaccurate or out-of-date data or data which is excessive and not required by it.

Individuals may ask the Company to correct Personal Data relating to them which they

consider to be inaccurate. If a member of staff receives such a request, then the rectification should be made. However, if staff do not agree that the Personal Data held is inaccurate, they should rectify but also record the fact that it is disputed and inform our Data Protection Officer.

Personal Data deemed inaccurate shall be rectified or erased within thirty (30) days of the individual's request.

Staff must ensure that Personal Data held by the Company relating to them is accurate and updated as required. If personal details or circumstances change, staff should inform the HR Department so that Company records can be updated.

10. Timely Processing

The Company will not keep Personal Data longer than is necessary for the purpose or purposes for which it was collected.

The Company will take all reasonable steps to destroy, or erase from its systems, all Personal Data which is no longer required.

Personal Data may be retained for the periods set out in the Company's Register of Processing Activities.

11. Processing in line with Data Subject's Rights

Data Subjects Rights differ under the Data Protection Laws. The Company will Process all Personal Data in line with Data Subject rights which will depend on the jurisdiction.

UK and EU
Under the UK and EU GDPR, the Company will comply with all Data Subject Rights set out below:

(a) Confirmation as to whether or not Personal Data concerning the individual is being Processed;

(b) Request access to any data held about them by a Data Controller (see also Clause 15 Subject Access Requests);

(c) Request rectification, erasure or restriction on Processing of their Personal Data;

(d) Lodge a complaint with a relevant supervisory authority;

(e) Data portability;

(f) Object to Processing including for direct marketing; and

(g) Not be subject to automated decision making including profiling in certain circumstances.

The Company shall respond to access and correction requests within thirty (30) days of receipt, and to withdrawal of consent requests within ten (10) business days of receipt.

The Company has also set out a Data Subject complaints procedure for Processing of Personal Data under the DPA 2018 (see Appendix 2).

Singapore
Under the PDPA, The Company will comply with all Data Subject Rights set out below:

(a) Request access to Personal Data about them that is in the Company's possession or under its control, as well as information about the ways in which such Personal Data has been or may have been used or disclosed within the year preceding the date of the request (the Company may charge a reasonable fee for actioning such access requests);

(b) Request correction of any error or omission in the Personal Data held by the Company, save where the Company is not required to make such correction pursuant to the Sixth Schedule of the PDPA; and

(c) Withdraw consent to the collection, use or disclosure of their Personal Data by giving the Company reasonable notice.

United States
Depending on the state in which a Data Subject resides, they may have certain additional privacy rights regarding their Personal Data. For example, U.S. state privacy laws currently enacted, including but not limited to the FDBR, and the privacy laws enacted in California, Colorado, Connecticut, Delaware, Florida, and Oregon, provide Data Subjects with privacy rights that may include:

(a) The right to confirm whether the Company is Processing their Personal Data and to access such Personal Data and the categories of Personal Data currently being Processed or that have been Processed;

(b) The right to obtain a copy of their Personal Data that was collected from and / or about them in a portable and, to the extent technically feasible, readily usable format that allows them to transmit the information to another Data Controller without hindrance, where the Processing is carried out by automated means;

(c) The right to obtain a list of specific third parties to which the Company has disclosed their Personal Data (unless the Company does not maintain this information in a format specific to the Data Subject, in which case, the Company will provide a list of specific third parties to which the Company has disclosed any Data Subject’s Personal Data);

(d) The right to obtain a list of categories of third parties to which the Company has disclosed their Personal Data;

(e) The right to delete Personal Data that the Company collected from and/or about them, subject to certain exceptions;

(f) The right to correct inaccurate Personal Data that the Company maintains about them, subject to certain exceptions;

(g) The right, if applicable, to opt out of the Processing of their Personal Data for purposes of (1) targeted advertising; (2) the “sale” of your Personal Data (as that term is defined by applicable U.S. state privacy law); and (3) profiling in furtherance of decisions that produce legal or similarly significant effects concerning them;

(h) If their Personal Data is profiled in furtherance of decisions that produce legal or similarly significant effects concerning them, the right to question the result of the profiling, to be informed of the reason that the profiling resulted in the decision, and, if feasible, to be informed of what actions the Company might have taken to secure a different decision

(and the actions that you might take to secure a different decision in the future). If applicable, the Data Subject also has the right to review the Personal Data used in the profiling and, if the decision is determined to have been based upon inaccurate Personal Data, the right to have the data corrected and the profiling decision reevaluated based upon the corrected data;

(i) The right to withdraw their consent if the Company is required by applicable law to obtain their consent to Process Special Categories of Personal Data;

(j) The right to designate an authorised agent to submit a consumer rights request on their behalf. The Company reserves the right to require written proof of authorisation and to verify the identity of both the Data Subject and the authorised agent before acting on any such request;

(k) The right not to receive discriminatory treatment by the Company for the exercise of their privacy rights; and

(l) The right to appeal the Company's decision in response to a consumer rights request. The Company will acknowledge receipt of any appeal and provide a written response within the timeframe required by applicable law (and in any event within 60 days of receipt). If the appeal is denied, the Company will inform the individual of their right to contact the relevant regulatory authority in their state, including the Florida AG for Florida residents.

Further information about U.S. requirements and Data Subject Rights is provided in Appendix 4 of the Privacy Policy. The Company's website and services are not intended for individuals under 16 years of age, and the Company does not knowingly collect, use, or disclose personal information from individuals under 16.

The Company shall respond to consumer rights requests within 45 days of receipt. Where a request is complex or numerous, this period may be extended by a further 45 days, in which case the Company shall notify the Data Subject of the extension and the reasons for it before the expiry of the initial 45-day period.

12. Data Security

The Company will take appropriate security measures against unlawful or unauthorised Processing of Personal Data, and against the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of or access to Personal Data transmitted, stored or otherwise Processed.

The Company will put in place procedures and technologies to maintain the security of all Personal Data from the point of the determination of the means for Processing and point of data collection to the point of destruction.

Personal Data will only be transferred to a Data Processor if the Data Processor agrees to comply with those procedures and policies, or if the Data Processor puts in place adequate measures itself. Staff should consult the Data Protection Officer to discuss the necessary steps to ensure compliance when setting up any new agreement or altering any existing agreement with a Data Processor.

Advice should also be sought from the Data Protection Officer as to whether a Data Protection Impact Assessment is required with the implementation of any new systems or software.

The Company will maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality means that only people who are authorised to use the data can access it;

(b) Integrity means that Personal Data should be accurate and suitable for the purpose for which it is Processed;

(c) Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal Data should therefore be stored on the Company's central computer system instead of individual PCs.

Security procedures include:

(a) Entry controls. Any stranger seen in entry-controlled areas should be reported;

(b) Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind (Personal Data is always considered confidential).

(c) Data minimisation;

(d) Pseudonymisation and encryption of data;

(e) Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required;

(f) Equipment. Staff must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC at the end of the day or at the end of their shift. The screens of People Team members are to be covered with filters; and

(g) Transferring Personal Data Outside of its original jurisdiction.

The Company may transfer any Personal Data it holds to a country outside of the UK and/or EEA or to an international organisation, provided that one of the following conditions applies:

(a) The country to which the Personal Data are transferred ensures an adequate level of protection for the Data Subjects' rights and freedoms;

(b) The Data Subject has given his consent;

(c) The transfer is necessary for one of the reasons set out in the Data Protection Laws, including the performance of a contract between the Company and the Data Subject, or to protect the vital interests of the Data Subject;

(d) The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims;

(e) The transfer is authorised by the relevant data protection authority where the Company has adduced adequate safeguards with respect to the protection of the Data Subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

Subject to the requirements above, Personal Data the Company holds may also be Processed by staff operating outside the UK and/or EEA who work for the Company or for one of its suppliers. Those staff may be engaged in, among other things, the fulfilment of contracts with the Data Subject, the Processing of payment details and the provision of support services.

The Company shall not transfer the Personal Data of individuals in Singapore to a country or

territory outside Singapore unless the Company has taken appropriate steps to ensure that:

(a) the recipient of the Personal Data is bound by legally enforceable obligations to provide a standard of protection to the transferred Personal Data that is at least comparable to the protection afforded under the PDPA; or

(b) the transfer is otherwise permitted under the PDPA.

13. Disclosure and Sharing of Personal Data, including International Data Transfers

The Company may share the Personal Data it holds with any member of its group, which means its subsidiaries, its ultimate holding company and its subsidiaries. The Company also operates internationally and transfers information to and from the UK, EU, United States, Singapore and UAE for the purposes described in this Policy.

For any transfers of Personal Data from the EU or UK, the Company uses appropriate safeguards, including relevant data security safeguards noted in this Policy and, when appropriate, the use of standard contractual clauses (SCCs) approved by the European Commission (for EU-origin transfers) or the UK International Data Transfer Agreement or equivalent addendum (for UK-origin transfers), as applicable. The Company shall provide a copy of the safeguards to individuals who inquire at privacyenquiries@aerfin.com.

The United States may have privacy and data protection laws that differ from, and are potentially less protective than, the data protection and privacy laws of other countries. Individuals' Personal Data can be subject to access requests from governments, courts, or law enforcement in the United States according to the laws of the United States.

14. Subject Access Requests

Individuals may make a formal request for the information we hold about them. Employees who receive such a request should forward it to the Data Protection Officer immediately.

When receiving telephone enquiries, staff will only disclose Personal Data held on the Company's systems if the following conditions are met:

(a) The caller's identity is checked to make sure that Personal Data is only given to a person who is entitled to it; or

(b) It is suggested that the caller put their request in writing if the caller's identity cannot be confirmed or checked.

Where a request is made electronically, data will be provided electronically where possible.

The Company will conduct reasonable and proportionate searches of a Data Subject's Personal Data if the request is made under the UK GDPR.

The Company's employees will refer a request to their line manager or the Data Protection Officer for assistance in difficult situations.

15. Reporting Personal Data breaches and breach procedure

Staff have a legal obligation to report any actual or potential data protection breach to the Data Protection Officer.

On receipt of any such report, the Data Protection Officer shall follow the breach procedure set out in Schedule 1 to this Data Protection Policy.

The Company acknowledges that it may have an obligation to report a data breach:

- to the ICO (in the UK) and/or the DPC (in Ireland) where such breach is likely to pose a risk to the rights and freedoms of the Data Subject. Risk being significant physical, material or non-material harm. Where it is determined to likely pose a high risk, the Company must also notify the affected Data Subjects without undue delay.

- to the PDPC (in Singapore) where the breach: (a) results in, or is likely to result in, significant harm to affected individuals; or (b) is of a significant scale, affecting five hundred (500) or more individuals. Where such a breach results in, or is likely to result in, significant harm to affected individuals, the Company shall also notify the affected Data Subjects as soon as practicable.

- to the Florida AG (in Florida) and affected Florida residents where the breach affects 500 or more Florida residents, irrespective of the risk level of such a breach. The Company shall also notify major nationwide consumer reporting agencies where 1,000 or more individuals are notified simultaneously.

The requirements for notification to relevant supervisory authorities and Data Subjects are explained in further detail in Appendix 1.

Any breach or non-compliance of the Data Protection Laws or this Policy by an employee will be dealt with through the Company's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

16. Contact details for queries or complaints

In case of any queries or questions in relation to this Policy, please contact the Data Protection Officer. Details below:

In case of **AerFin Limited**:
privacyenquiries@aerfin.com
with copy to
Naomi Mattock
Address: Newton Road, Crawley
RH10 9TS
Tel: +44 1293 583244
Email:
naomi.mattock@aerfin.com

In case of **AerFin Limited (Singapore Branch)**:
privacyenquiries@aerfin.com
with copy to
Jo Rival
Address: 105 Cecil street, #18-18,
The Octagon, Singapore, 069534
Tel: +44 7867 336617
Email: jo.rival@aerfin.com

In case of **AerFin US, LLC:**
privacyenquiries@aerfin.com with copy to
Naomi Mattock
Address: 3740 West 104th Street, Hialeah, FL 33018, United States
Email:
naomi.mattock@aerfin.com

17. Complaints

The Company shall endeavour to handle all complaints related to data protection in the first instance. Irrespective of this, the Company acknowledges that Data Subjects have the right to complain to the relevant supervisory authority (i.e., ICO, PDPC, DPC, Florida AG, etc.) about the Processing of their Personal Data.

Under the DPA 2018, we are required to have a procedure in place for handling data protection related complaints. Any complaints from Data Subjects in relation to how we Process their Personal Data that is within scope of the DPA 2018 / UK GDPR will be handled in accordance with the procedure set out in Appendix 2.

Individuals in the U.S. also have the right to contact the Federal Trade Commission (reportfraud.ftc.gov) in respect of federal consumer protection matters. Where a U.S. Consumer's rights request is denied in whole or in part, the Consumer may submit an appeal to the Company using the contact details set out in Section 16. The Company shall acknowledge receipt of the appeal and provide a written response within 60 days. If the appeal is denied, the Company will notify the Consumer of their right to contact the Florida AG.

18. Training

Annual data protection training will be required to be undertaken by all Company staff. The Company shall keep a record of the individuals who have completed such training.

19. Updates to this Policy

We regularly review and, if appropriate, update this Policy from time to time, and as our services and use of Personal Data evolves. We will update the date of this document each time it is changed.

AerFin

Appendix 1: Personal Data Breach Procedure

1. Data Protection Officer is notified of a Personal Data breach (or potential breach) by a member of staff (or other third party);

2. Data Protection Officer records the date and time of the receipt of such notification;

3. Data Protection Officer co-ordinates a call with the data protection task force which consists of the following AerFin officers (and any other individual that the Data Protection Officer deems necessary on a case by case basis) ("**Data Protection Task Force**") to raise awareness of the breach:

    - Chief People Officer
    - VP Legal
    - People Manager
    - IT & Transformation Director
    - Chief Financial Officer

4. During the call, the Data Protection Task Force shall consider the actions to be taken in response to the breach and shall allocate associated responsibilities as set out in the table below.
5. Data Protection Officer shall be responsible for co-operating with the relevant data protection regulator (as applicable) and for co-ordinating any further actions with Data Protection Task Force.

Action	Responsibility
Do we need to report the breach to the relevant supervisory authority? *ICO / DPC* Breaches need only be reported to the ICO / DPC if the data breach is likely to result in a risk to the Data Subject's rights and freedoms. Risk is defined as physical, material or non-material harm. The following risk assessment should be carried out to determine whether the breach is reportable: UK GDPR data breach reporting (DPA 2018) | ICO *PDPC* A data breach must be reported to the PDPC if it: (a) results in, or is likely to result in, significant harm to affected individuals; or (b) affects, or is likely to affect, five hundred (500) or more individuals. *FIPA* A data breach must be reported to the Florida AG if affects 500 or more Florida residents. It must also be reported to major nationwide consumer reporting agencies where 1,000 or more individuals are notified simultaneously.	Data Protection Officer

If the breach is reportable – inform the relevant supervisory authority (as applicable) The following information will be required and should be provided by the relevant members of the Data Protection Task Force: - What has happened? - When and how we found out about the breach. - The people that have been affected by the breach. - What are we doing as a result of the breach? - Contact details to be provided to the relevant supervisory authority (which will be the Data Protection Officer). **If it is determined that the breach is not reportable, the breach needs to be logged on internal breach register in any event.** *ICO / DPC* The ICO/DPC must be notified within 72 hours of discovery of the breach. The ICO can be notified using the following form: UK GDPR data breach reporting (DPA 2018) | ICO The DPC can be notified by clicking the following: DPC Breach Notification *PDPC* The PDPC must be notified as soon as practicable, and in any event no later than three (3) calendar days after the Company has assessed that the breach is a notifiable data breach under the PDPA. The PDPC can be notified via the PDPC's data breach notification form available at www.pdpc.gov.sg. *FIPA* The Florida AG must be notified within 30 days of discovering or reasonably believing a breach has occurred, extendable to 60 days upon written request to the Florida AG.	Data Protection Officer
What needs to be done immediately to mitigate the risk associated with the breach?	Data Protection Task Force as a whole.
Do we need to notify affected Data Subjects? Under the UK and EU GDPR, affected Data Subjects need to be notified if it is found that the data breach is likely to result in a high risk to their rights and freedoms.	Data Protection Officer, VP Legal, Chief People Officer, People Manager

Under the PDPA, where such a breach results in, or is likely to result in, significant harm to Data Subjects and the Company shall notify the Data Subjects as soon as practicable. Under FIPA, where such a breach affects 500 or more Florida Residents (irrespective of any risk assessment), with notification being without unreasonable delay.	
Data Protection Task Force to determine the following: - Do we know how this breach happened? - What are we going to do about it? - Do we know how to fix it? - Are any third party service providers involved?	Data Protection Task Force to allocate actions as are appropriate in the circumstances.
Schedule follow up calls to monitor progress on actions	Data Protection Officer
Depending on severity of the breach – inform insurers.	Data Protection Officer

Appendix 2: Complaints Procedure

(a) Raising a complaint

Any Data Subject who believes their Personal Data has been mishandled in a way that contravenes the DPA 2018 or UK GDPR by the Company may submit a complaint. Common examples include complaints about:

- unlawful Processing of Personal Data;
- failure to respect Data Subject rights;
- inadequate security measures; or
- non-compliance with data protection principles.

We encourage complaints made to us by contacting us as per Section 18 of this Policy and using a complaint form in Appendix 3. However, we acknowledge that Data Subjects can make a complaint to the Company by any means, including through social media. In these cases, we will ask for alternative contact details so we can respond to their complaint accordingly.

(b) Complaint handling

Step one: Receipt

Before acknowledging any complaint, the Company shall confirm:

- it is the Data Controller of the relevant Processing; and
- the identity of the individual, or the individual's representative.

Step two: Acknowledgement

We will aim to acknowledge complaints within 5 working days of receipt, and in any event no later than 30 calendar days.

Where we do not understand the nature of the complaint, we may need to ask the Data Subject to put the complaint in writing so that we are sure we are responding appropriately. We are also required to ensure the identity of the complainant, and therefore we may ask for further information or documentation to verify the Data Subject's identity if we cannot do so initially.

Step three: Investigate

We will investigate the complaint as soon as practicable after receipt and acknowledgement. This includes:

- reviewing all relevant documentation;
- consulting with relevant colleagues and teams; and
- gathering evidence to determine whether either the DPA 2018 or UK GDPR has been contravened.

Step four: Outcome

We aim to investigate and provide a response to the complaint within one month. This response may include:

- what information has been found by the Company; and
- whether the complaint is upheld or not, and if it is, any corrective actions we have taken or will take.

Where the complaint is complex or particularly challenging, we will inform the Data Subject as soon as possible and keep them informed of any progress, as appropriate.

If the Data Subject is happy with our response, the Company may consider either clarifying / following up our response or confirming that the complaint has been closed.

(c) Documentation

The Company will endeavour to keep records that evidence our compliance with this complaints procedure, including:

- the date we received the complaint;
- the Company's acknowledgement communication;
- any relevant conversations and documentation while investigating;
- the outcome of the complaint, including any actions taken as a result of the investigation.

(d) Right to escalate

The Data Subject has the right to complain directly to the ICO at any point, including during our complaints procedure process. The Company shall ensure it has made the Data Subject aware of their right to complain to the ICO.

AerFin

Appendix 3: Data protection complaint form

[Your full address]

[Phone number]

[date]

[Name and address of AerFin entity]

[Reference number (if we gave you one)]

Dear [Sir or Madam / name of the person you have been in contact with]

Data protection complaint

[Provide your full name and address and any other details such as account number so we could identify you]

[Give details of your complaint clearly and simply and, if needed, its effect on you.]

Please respond fully within one calendar month. If you can't reply within that time, please tell me when you will be able to reply.

If you'd like to discuss this, please contact me on [telephone number / email address].

Yours sincerely,

[Name]

[Signature]