Code of Conduct – Personal Data Protection

Nordic Aviation Capital

NAC Corporate Legal/ Compliance

Issued 1 November 2022

Introduction and Purpose

NAC processes personal data and is therefore subject to various data protection and privacy laws and regulations. NAC is committed to international compliance with personal data protection laws and respecting individual privacy. Improper processing of personal data, or other violations of personal data protection laws, can result in significant fines and claims for damages against the company. Ensuring personal data protection is the foundation of trustworthy business and the reputation of NAC. As such, violations for which NAC Personnel are responsible will be taken very seriously.

Personal data is any information relating to a directly or indirectly identifiable person and can include, but is not limited to, name, home address, contact information and pay and benefits.

NAC's Personal Data Protection Policy (the "**Policy**") sets out rules and procedures for processing personal data, including cross-border transfers of personal data throughout NAC regions, to ensure that NAC protects personal data from unauthorised access, distribution or use.

The Policy applies to all persons employed by NAC, contractors and any member of the Board while acting for NAC ("**NAC Personnel**") and to all NAC regions. It is applicable to contacts between NAC Personnel internally and with third parties. For example, it applies to:

- Processing of officer, employee and contractor information (including potential and former officers, employees and contractors) and HR information.
- Processing of information relating to KYC or KYS procedures.
- Processing of business contact and related information on the employees, officers and advisors of business counterparties and suppliers.

Any unauthorized processing of personal data by NAC Personnel is prohibited. NAC Personnel may not use personal data for private or commercial purposes, or otherwise disclose or make available such information to unauthorized third parties. Each head of department must inform new NAC Personnel in their team about the obligation to protect personal data and this Code of Conduct and the Policy. The obligation to protect personal data that arises from an employment /contractual relationship with NAC continues even after that employment has ended.

Transparency and Employee Privacy Notice

NAC will establish and follow procedures to ensure that data subjects are provided with information regarding how and why NAC processes their personal data before or as soon as possible after the processing begins.

NAC Personnel are periodically sent information about the processing of their personal data through NAC's data protection notice (the "Employee Privacy Notice"). NAC Personnel should be provided with information separately about any additional processing systems which affect them and are not already covered by the Employee Privacy Notice.

Personal data should be collected and processed fairly for specified, express and legitimate purposes. NAC will not process personal data in ways which are incompatible with the purposes for which they were collected.

Sensitive Personal Data

You should take particular care in relation to the processing of personal data in the following, sensitive categories ("**Sensitive Personal Data**"):

- Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership.
- Genetic data and biometric data processed for the purpose of uniquely identifying a living individual.
- Personal data concerning a living individual's health, sex life or sexual orientation; and
- Personal data relating to criminal convictions and offences or related security measures.

NAC will only process Sensitive Personal Data where the data subject has given their explicit consent and in accordance with applicable laws, or where the Compliance Team has approved the processing in writing (assuming explicit consent not required).

Transfer of Personal Data to Third Parties and International Data Transfer

Any disclosure of personal data to third parties must meet all the requirements of the Policy. Please note that disclosure will include circumstances in which an individual in one country has remote access to personal data stored or processed in another country. NAC will consider whether it is appropriate to impose data privacy obligations on a third party before transferring personal data to it.

NAC's establishments in the will only transmit personal data outside to another country in accordance with the Policy.

Updating, Retention and Destruction

NAC will take reasonable steps to ensure that all personal data is accurate and, where relevant, up to date. NAC will delete or anonymise personal data when they are no longer needed given the purposes for which they were collected and are processed.

Data Security

Technical and organisational security measures will be put in place to protect all personal data processed at NAC to mitigate risks associated with their accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

NAC is required to report certain breaches of security affecting personal data to the relevant data protection authorities and in some circumstances may also be required to inform the affected data subjects within a certain timeframe.

Rights of Data Subjects

Data Subjects have the right to:

- receive a copy of any personal data that NAC holds about them, with certain related information.
- require NAC to update, complete or correct any inaccurate or incomplete personal data concerning them without undue delay.
- require NAC to stop processing their personal data for direct marketing purposes, if done; and

- object to the processing of their personal data more generally.

Data Subjects may also have the right, in certain circumstances to:

- require NAC to delete their personal data without undue delay.
- limit NAC's processing of their personal data, so that it can only continue subject to very tight restrictions.
- require personal data which they have provided to NAC, and which are processed based on their consent or the performance of a contract with them, to be "ported" to them or a replacement service provider; and
- request information on the public and private entities with whom NAC has shared their personal data.

Co-operation with Authorities

NAC is required to co-operate with competent data protection authorities. Any communication received from a data protection authority should be passed to the Compliance Team.

Reporting and Training

Whilst the Board (with support from the General Counsel and Compliance Team) has overall responsibility for ensuring compliance with this Code of Conduct and the Policy by NAC and NAC Personnel, all NAC Personnel has the responsibility for compliance and familiarising themselves with this Code of Conduct and related policies.

NAC's compliance program includes training (both initial and ongoing mandatory annual training), updates and the monitoring of compliance with the Policy. NAC's Compliance Team will also deal with any internal queries and audit internal control systems and procedures (in cooperation with the General Counsel and Chief Risk Officer) to ensure that they are effective.

Reporting will be a crucial part of the Policy's awareness program. If NAC Personnel become aware of, or suspect that, a breach of law or this Code of Conduct or the Policy has occurred, they must promptly report via the appropriate internal channels (including their manager, the next most senior supervisor, or the NAC Compliance Team), and/ or via the confidential external hotline (contact details for which can be found in the "Policies & Handbooks" section on the Corporate Hub).

NAC Personnel raising concerns in accordance with the Policy will not be subjected to retaliation or penalised in any way for raising a concern. NAC will not tolerate retaliation against individuals who raise matters under this Code of Conduct, or the Policy and instances of retaliation will be taken seriously and addressed appropriately.

Please also refer to NAC's Global Whistleblowing Policy concerning reporting generally.

Consequences For Failure to Comply

Failure to comply with applicable laws and regulations are serious offences and strictly prohibited both by law and by the Code of Conduct. NAC Personnel who act in breach of this Code of Conduct or the related Policies may be subjected to disciplinary measures, up to and including dismissal. They may also risk being prosecuted by the criminal prosecution authorities.

For further information, please refer to NAC's other codes of conduct and compliance policies, available in the "Policies & Handbooks" section on the Corporate Hub.