

Code of Conduct

Corymbia Group

Document Information

Scope of application

This Code of Conduct applies to all employees of Corymbia GmbH and its affiliated companies, namely HPC2 Asset GmbH, as well as to all suppliers to the best extent possible.

Policy owner

Board of Directors

Entry into force

March 2025

Document history

Version	Date	Author	Changes / Comment	Approved by
1	02/2025	Joanna Burke	Initial version	Board of Directors

Contents

Code of Conduct	1
1. Glossary	4
2. Code of Conduct	6
2.1 Overview	6
2.3 Conflicts of Interest	8
2.4 Whistleblower Policy.....	9
2.5 Anti-competition.....	9
2.6 Cybersecurity, Data Protection, and Privacy.....	10
2.7 Corruption and Fraud	11
2.8 Implementation.....	11

1. Glossary

ESG (environmental, social and governance)

ESG refers to a broad framework used to evaluate a company's performance beyond financial (and often shorter-term) metrics, measuring direct and indirect inputs and outputs.

Environment: this aspect of ESG relates to the impact of a company on the environment, including with regards to issues such as carbon emissions, resource use & efficiency, and waste management.

Social: this pillar refers to the company's relationships with its key stakeholders, such as employees, customers, and communities where it operates. It includes topics such as human rights and diversity, equity and inclusion (DEI).

Governance: this aspect refers to internal systems, processes and controls a company has in place to operate. It includes topics such as business ethics, shareholder rights, and cybersecurity.

EU Minimum Social Safeguards

The EU Taxonomy Minimum Social Safeguards (MSS) criteria work to ensure that entities carrying out environmentally sustainable activities (labelled as Taxonomy-aligned) meet certain minimum governance standards and do not violate social norms.

"The minimum safeguards . . . shall be procedures implemented by an undertaking that is carrying out an economic activity to ensure the alignment with the OECD Guidelines for Multinational Enterprises and the UN Guiding Principles on Business and Human Rights, including the principles and rights set out in the eight fundamental conventions identified in the Declaration of the International Labour Organisation on Fundamental Principles and Rights and work and the International Bill of Human Rights."

These criteria are assessed at the entity level and guidance focuses on investments in private and public entities incorporated as companies. The central aim is to ensure that entities respect human rights, labour rights, prevent bribery, tax evasion and unfair competition.

EU Whistleblower Directive (2019)

Legislative act with the primary aim of establishing common minimum standards for the protection of individuals who report breaches of Union law in the public interest. The directive mandates secure and confidential reporting channels, protection for whistleblowers, and obligations for organisations to handle whistleblower reports effectively.

Global Reporting Initiative

A comprehensive framework for sustainability reporting, enabling organisations to disclose their economic, environmental, and social performance.

International Bill of Human Rights

A comprehensive list of Human Rights, which includes the Universal Declaration of Human Rights, International Covenant on Economic Social and Cultural Rights (ICCPR) and the International Covenant on Civil and Political Rights (ICESCR). Companies can align with the ICCPR and ICESCR by ensuring provision of the rights listed on this webpage.

International Finance Corporation (IFC) Performance Standards on Environmental and Social Sustainability	The <u>Performance Standards</u> provide guidance for entities making investments on how to identify investee company environmental and social risks and impacts and mitigate them. It contains 8 performance standards which must be aligned with, including Assessment and Management of Environmental and Social Risks and Impacts, Labor and Working Conditions, Resource Efficiency and Pollution Prevention, Community Health, Safety, and Security, Land Acquisition and Involuntary Resettlement, Biodiversity Conservation and Sustainable Management of Living Natural Resources, Indigenous Peoples, and Cultural Heritage. To align, investee companies must co-operate with the investor to achieve the environmental and social standards set out in the framework.
International Labour Organisation (ILO) Core Conventions	Legally-binding legal instruments drawn up by <u>ILO</u> constituents (governments, employers and workers), that set out basic principles and rights at work. Basic human rights, occupational safety and health, wages, working time, employment policy and promotion, vocational guidance and training, skills development, specific categories of workers, labour administration and inspection, maternity protection and social security, indigenous and tribal people, and migrant workers are all work issues covered in the Core Conventions. Companies can incorporate the principles into their Codes of Conduct or other responsible business conduct initiatives.
Organisation for Economic Co-operation and Development (OECD) Guidelines for Multinational Enterprises	<u>Recommendations</u> addressed by governments to multinational enterprises, which aim to encourage positive contributions enterprises can make to economic, environmental and social progress, while minimising adverse impacts. The guidelines cover areas such as climate change, biodiversity, business responsibility, human rights, etc. Enterprises can align by focusing on responsible business practices such as setting climate and biodiversity goals, using data and technology responsibly, and having robust anti-corruption measures in place.
The Treaty on the Functioning of the European Union (TFEU)	The <u>TFEU</u> is one of two treaties forming the constitutional basis of the European Union, alongside the Treaty on European Union (TEU). As stated in its introductory clause, the purpose is to “lay the foundations of an ever closer union among the peoples of Europe”, and its Part 3 (Articles 26 to 197) comprising of the largest section stipulates the legal basis for EU policies and internal actions regarding areas such as, but not limited to, free movement of goods; competition, taxation, and the harmonisation of legislation; employment policy; social policy; consumer protection; and civil protection.
United Nations (UN) Global Compact (UNGC)	A global <u>corporate sustainability initiative</u> which calls on companies (among other entities) to align their operations and strategies with environmental, human rights, labour and anti-corruption principles. To join the UNGC, companies must align with the outlined universal sustainability principles, following through with associated actions and reporting. The membership fee is \$30,000 per annum, meaning it may not be suitable for smaller companies, but the principles could still be used as a guide.
UN Guiding Principles on Business and Human Rights	The <u>Guiding Principles</u> seek to provide an authoritative global standard for preventing and addressing the risk of adverse human rights impacts linked to business activity. Enterprises should seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships.

2. Code of Conduct

2.1 Overview

Guiding Principles

Corymbia and its affiliated companies are committed to conducting business with ethical integrity.

The following Code of Conduct (“the Code”) demonstrates our commitment to responsible policies and practices in the workplace, which, in practice, means investment in the welfare of our employees and being a responsible actor both locally and globally. Corymbia’s central guiding principles which shape the approach to all business activities and operations are as follows:

1. Integrity – Acting with ethical integrity at all times in all internal and external interactions.
2. Respect – Treating everyone with fairness and dignity without discrimination and with respect of diverse opinions and beliefs.
3. Accountability – Holding ourselves and each other accountable as well as maintaining responsibility of the impact of our actions on others and the environment.
4. Transparency – Behaving truthfully and transparently in our communications and actions at all times. In parallel, respecting confidentiality when and as needed.

Structure of Document

The Code outlined below aims to establish a fundamental set of principles and a practical process for Corymbia to ensure consistency in its moral standards and interactions with relevant stakeholders. The Code addresses the following topics:

- Expectations for key stakeholder groups
- Conflicts of Interest
- Whistleblower Policy
- Anti-competition
- Cybersecurity, Data protection, and Privacy
- Corruption and Fraud

Introductory Remarks

The Code is reviewed annually by the Board of Directors.

Compliance with the Code is mandated for all employees and relevant third-parties, i.e., governance bodies, employees, consultants, vendors, clients and all other third-parties. Ensuring compliance, and by extension, local laws and regulations, helps Corymbia to mitigate regulatory, corporate, reputational and corporate risks and build trust with relevant stakeholders. This justifies our ‘license to operate’ and aims to bring positive impacts to our employees, customers and the wider community.

Any potential violations of the Code must be communicated to the Board of Directors, and any non-adherence to Corymbia’s Code will result in disciplinary action. We appreciate your support in collectively ensuring that our values are continuously upheld.

2.2 Stakeholder Commitments and Behaviours

This Code has a broad application across three key stakeholder groups, namely; Senior Management, All Employees and External Stakeholders, with the intention of supporting and enhancing Corymbia's 'license to operate'.

Social License to Operate

In all locations where Corymbia has operational business activities, our operations should minimise negative environmental, economic and social impacts. At minimum, this entails complying with the relevant ESG regulations applicable to each location.

Through actions detailed in documents such as our Sustainability Policy, the Company maintains accountability of the effects of our actions across all parties directly and indirectly involved. Expectations required to achieve a license to operate are detailed below.

Senior Management (including Board Members)

All members of this stakeholder group are expected to:

- Ensure collective understanding of the Code across the company by forming onboarding and training structures.
- Ensure guidance for the Code is up to date and reviewed regularly.
- Establish a monitoring and escalation procedure for the Code.
- Provide an anonymous and safe reporting mechanism for any issues identified relating to the requirements of the Code.
- Ensure accountability for upholding the Code within the governance body.
- Members of the governance body must also adhere to all employee expectations outlined.

All Employees

All members of this stakeholder group are expected to:

- Read and ensure full understanding of the Code.
- All employees in management positions must understand all relevant regulations in the jurisdictions the companies operates in, including Anti-Corruption and Modern Slavery laws.
- All employees must treat each other with equality, fairness and respect. (Company) has zero-tolerance to discrimination, harassment, and bullying in the workplace.
- All employees must uphold environmental responsibility, as detailed in the Sustainability Policy.
- All employees must maintain professional standards in all public communication as a representative of (Company).
- This extends to all interactions with external stakeholders.

External Stakeholders

- All external stakeholders should be made aware of the Code and related policies and are expected to uphold the Company's values.
- The Company's Supplier Code of Conduct contains additional details on requirements for external stakeholders.

2.3 Conflicts of Interest

The Global Reporting Initiative defines Conflicts of Interest as a "situation where an individual is confronted with choosing between the requirements of their function in the organisation and their other personal or professional interests or responsibilities"¹. At Corymbia, we firmly believe that instances of conflicts of interest are detrimental to the equitable running of the company, and therefore, strive to ensure that any such instances are prevented and mitigated.

It is important to note the demarcation between actual, perceived, and potential conflicts of interest as The Ethics Institute defines²:

- "Actual conflicts of interest are where my personal interests are in real conflict with my official responsibilities. An example of this is where I am on an interview panel and my child has applied for the position."
- "Perceived, or apparent conflicts of interest are where it may reasonably seem to an independent third party that a conflict of interest exists, whether or not this is actually the case. An example of a perceived conflict of interest would be where a government minister's son is awarded a contract in the minister's department, even though due process was followed."
- "Potential conflicts of interest are where there is not currently a conflict of interest, but if something changes there is the likelihood that one may arise. An example of this would be to have the possibility to be promoted into a position where you will be the relationship manager with your cousin's company. There is currently no conflict, but it may come into play if circumstances change."

Employees should be vigilant to recognising all three degrees of conflicts of interest, as actual ethical activity and perception of ethical reputation in the long-term are equally pertinent to a successful, sustainable business.

As such, procedures and accountability mechanisms shall be established and will be followed where practicable to ensure standards are upheld throughout Corymbia against instances of actual, perceived, and potential conflicts of interest in alignment with the Reporting Mechanism.

Employees which suspect any misconduct related to this matter should use the same escalation mechanism as listed at the end of the Code's Overview section. For instances where an employee is unsure as to whether an action may breach such standards, ensure to raise concerns to your direct line of manager in the first instance.

¹ GRI 2 General Disclosures: globalreporting.org/publications/documents/english/gri-2-general-disclosures-2021/

² [Conflict-of-Interest-Handbook eBook.pdf \(tei.org.za\)](#)

2.4 Whistleblower Policy

Whistleblowing is defined as the act of an employee disclosing suspected wrongdoings or illegal activities at work. This policy section aims to outline a process which ensures that everyone employed at Corymbia should feel confident and safe in speaking up regarding any issues themselves or others are facing.

Corymbia is committed to transparency and accountability as defined by international standards³, and accordingly, we enforce procedural mechanisms to facilitate communication and protection from retaliation⁴.

The Policy commits to the establishment of a secure reporting channel and a procedure for follow-up as defined by the Directive. Whistleblowers will have at their disposal effective channels to report suspected breaches of confidentiality, both internally (within an organisation) and externally (to a competent authority). Their reports will be properly investigated and acted upon by the organisations and competent authorities.

The reporting and follow-up processes will comply with the below:

- Corymbia shall establish a reporting mechanism such that the whistleblower may report in writing and/or orally. This may be in the form of an anonymous online survey form, whistleblowing hotline, or if requested, a physical meeting shall be conducted within a reasonable timeframe.
- The confidentiality of the whistleblower and any third party mentioned in the whistleblowing report shall be protected. The report must only be accessible to authorised individuals.
- Acknowledgement of receipt shall be communicated to the whistleblower within seven days of submission.
- Impartial communication and feedback by a designated personnel shall be provided within three months from acknowledgement of receipt. This personnel shall provide diligent follow-up in a timely manner and as needed.
- The whistleblower shall be allowed to review and revise the initially submitted report and interview notes, as the investigation proceeds.

Employees or stakeholder which suspect any misconduct related to the items listed above should contact their direct line manager or relationship manager to raise concerns in the first instance. The Board of Directors is also always available to discuss such matters.

2.5 Anti-competition

Corymbia does not tolerate any unfair methods of competition and deceptive acts or practices as per our commitment to the OECD Guidelines for Multinational Enterprises and the EU Minimum Social Safeguards. We conduct all business activities with ethicality and integrity, including adherence to free and fair competition in alignment with competition policies within The Treaty on the Functioning of the European Union (TFEU) as a minimum standard. We value the maintenance of trusting and sustainable relationships with our business

³ Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law. The 2019 EU Whistleblower Protection Directive outlines a minimum standard to enforce procedural mechanisms for Whistleblower Protection.

⁴ "Retaliation" is defined by Article 5.11 of the Directive as "any direct or indirect act or omission which occurs in a work-related context, is prompted by internal or external reporting or by public disclosure, and which causes or may cause unjustified detriment to the reporting person".

partners, suppliers, and any other supply chain body. It is strictly prohibited any one individual in Corymbia or affiliated companies to engage in price fixing, market sharing, agreement on customer allocation, agreement on product limitation, distribution agreements between suppliers and re-sellers, and any other agreement and information exchange with competitors that can be seen as anti-competitive. The same conduct is expected throughout the supply chain.

Any infringement of these principles may lead to disciplinary measures, including the termination of an employment relationship or other legal proceedings. A suspected violation should be swiftly flagged via the Reporting Mechanism, as further detailed in “2.8 Implementation” below.

2.6 Cybersecurity, Data Protection, and Privacy

In an increasingly digitised world, led by the proliferation of mobile and Internet-of-Things (IoT) enabled devices, cloud computing, artificial intelligence (AI) and data sharing, cybersecurity and data protection are critical issues for Corymbia to address to ensure privacy, security, trust, and ultimately, business resilience.

Corymbia is compliant with relevant local or regional legislation⁵ concerned with data protection, and we are committed to managing and safeguarding sensitive information, and expect the same integrity by our employees and third parties alike.

“Data” refers to all employee data, customer data, supplier data, and data on sensitive projects. Employees are expected to utilise devices provided by the company and data should not be transferred to personal devices, unless in an exceptional circumstance where an employee will have been granted permission by a relevant management personnel. Corymbia commits to implementing the following measures:

- **Endpoint security:** ‘Zero Trust’ antivirus software for all devices in use in company operations, such as laptops, mobile phones, servers, and industrial IoT devices.
- **Network security:** cybersecurity software in the form of intrusion detection and protection systems, firewalls and encryption protocols contribute to the Company’s ‘Zero Trust’ stance towards actions taken on the company’s IT estate.
- **Access control:** data governance processes to ensure the correct permissions are in place for user access in relation to seniority, role type, etc. Identity verification software has been procured for identity verification and protection of sensitive data.
- **Incident response and recovery:** ensuring adequate processes and digital infrastructure is in place so that in the event of a cyber or other data security breach incident, response times, recovery plans, and communication procedures are in place to minimise risks.

Any employee who may suspect risk of a data breach or any other form of cybersecurity attack should notify upwards via line management/relationship management or a member of the Board of Directors.

⁵ Relevant legislation includes EU General Data Protection Regulation (GDPR) / the 2018 UK Data Protection Act / 1988 Australian Privacy Act / 2012 Singaporean Personal Data Protection Act (PDPA) or other similar forms of legislation in other geographic regions where the company operates.

2.7 Corruption and Fraud

Corymbia operates with a zero-tolerance policy regarding bribery, corruption, fraud, and any other criminal conduct in its operations and supply chain, upholding the values enshrined in Corymbia's Code for employees and Supplier Code of Conduct for suppliers. This includes money laundering, and Corymbia is committed to full compliance with tax duties in laws, regulations, and any other obligations that may be applicable to the respective local or regional context in each given business activity. We transparently cooperate with public authorities and report relevant information where required or requested.

The Company's Board of Directors is responsible for building awareness of the aforementioned risks and commits to the following actions to reduce these risks:

- Compliance with local and international anti-bribery and corruption laws.
- Implementation of an internal control system for the prevention of criminal and fraudulent activities, which is included in our internal and external confidential Whistleblowing and Reporting Mechanisms.
- Risk mapping and materiality analysis across Corymbia's operations and supply chain
- Due diligence and supplier questionnaire for all new clients, suppliers, and third-party partners.
- Periodic internal and external audits for actual and potential risks
- Internal controls such as duty segregation (separating financial roles to avoid one person with complete control over transactions) and approval processes for transactions. All employees are expected to adhere to the principles of law-abiding conduct and maintain awareness of such risks.
- Company policy that all documents (contracts, orders etc) must always be signed by 2 individuals in accordance with the Company delegation of authority matrix.

Where an employee or external stakeholder may suspect any potential criminal or fraudulent activity, it is their duty to immediately notify their direct line manager or relationship manager, or by way of discussing the matter with any member of the Board of Directors.

2.8 Implementation

Communication and Training

Corymbia will ensure to communicate the Code to all employees, senior management personnel and external stakeholders where appropriate.

All employees in managerial positions will also have ESG targets included in their performance reviews. Where appropriate external stakeholders will have ESG reporting obligations and/or targets.

Reporting Mechanism

Corymbia's employees and external stakeholders are responsible for ensuring the Code is upheld and an appropriate degree of penalty shall be enforced in cases of infringement. Depending on the severity of an identified infringement, possible consequences range from a written warning, removal of responsibilities, termination of employment, being sued for losses, or in extreme cases, being individually prosecuted.

The following steps should be taken if any potential incidents are encountered:

1. Reflect on the incident prior to taking any action to ensure you have a holistic understanding of the situation.
2. Reach out to others you are comfortable speaking with, including your line manager, a member of the Board of Directors or someone who may have been in a similar situation, to get a second opinion on the issue (keeping confidentiality as appropriate).
3. If escalation is deemed as required, formally report the incident to your line manager/relationship manager, or a member of the Board of Directors.
4. The Board of Directors will subsequently conduct an initial review of the reported content within 5 working days and confirm receipt.
5. If further information may be needed, a member of the Board of Directors will seek to arrange a meeting with the reporter within 15 working days from the day that receipt is confirmed.
6. Appropriate action for remediation and consequences will be determined by the Board of Directors.

Responsibility

It is the responsibility of all involved in the Companies operations to uphold the Code of Conduct.

The Board of Directors are ultimately accountable for the Code and it will be reviewed by the Board of Directors on an annual basis and updated as required.



Corymbia GmbH

Eschersheimer Landstraße 14

60322 Frankfurt am Main

HRB 180624