Values & Ethics

Doc no: EPS-MGM-0008, rev 02

Date: 10.07.2023

By: Fredrik Aarnes

Checked by:	Date:	Approved By:	Date:
Nina Hjartåker Nerland	03.07.2023	Tom Munkejord	10.07.2023

Revision History

Revision	Description
01	Document changed name from AKK 14
02	Included the Transparency Act

1 Purpose and Scope

The purpose of this document is to describe EUREKA GROUP's values and Code of Conduct, which are to form the basis for building a good culture and reputation in EUREKA GROUP. With this document, EUREKA GROUP confirm its commitment to ensure that its business practices as well as its partner relationships have a positive impact on the efficacy of and compliance with human rights, labour standards, environmental standards, and business integrity.

This document, combined with other governing documentation (EPS-MGM), describes how the group will handle its corporate social responsibility. This document is valid for all subsidiaries of EUREKA GROUP AS.

Contents

1 Purpose and Scope 2
2 Responsibility 6
3 Values 6
4 Code of Conduct 7
4.1 General 7
4.2 Business Ethics 7
4.3 Own behavior 8
4.4 Directorships and other work-related matters 9
4.5 Information and IT systems 9
4.6 Confidentiality 10
4.7 Bribes and corruption 10
4.8 Whistleblowing 11
4.9 Implementation 12
4.10 Consequences of violation 12
4.11 Guidelines for Sanctions of Compliance 12
4.12 Guidelines for Integrity Due diligence 13
5 Appendices 13
5.1 Appendix 1; Guidelines for Code of Conduct 14

5.1.1 Principle 1: We comply with the law 16
5.1.2 Principle 2: We respect our colleagues 17
5.1.3 Principle 3: We ensure healthy and safe working conditions 18
5.1.4 Principle 4: We protect our assets and confidential information 19
5.1.5 Principle 5: We respect fundamental human rights 20
5.1.6 Principle 6: We never make unlawful payments 22
5.1.7 Principle 7: We carefully choose our business partners 23
5.1.8 Principle 8: We avoid conflicts of interest 24
5.1.9 Principle 9: We compete fairly 25
5.1.10 Principle 10: We operate in an environmentally responsible manner 26
5.2 Appendix 2; Anti-Corruption Policy 27
5.2.1 What is corruption? 27
5.2.2 Bribes 27
5.2.3 Trading in influence 29
5.2.4 Palm greasing 29
5.2.5 Facilitation payments 29
5.2.6 Who is considered a public servant? 30
5.2.7 Further guidance on certain activities 31
5.2.7.1 Gifts and hospitality 31
5.2.7.2 Engagement of business partners 32
5.2.7.3 Work with agents 33
5.2.7.4 Joint ventures 34
5.2.7.5 Acquisitions 35
5.2.7.6 Social projects, donations and grants 35
5.2.8 Internal procedures 36
5.2.8.1 Risk assessments 36
5.2.8.2 Implementation and training 36
5.2.8.3 Monitoring and review 36
5.2.8.4 Handling of reports on violations 36
5.2.8.5 Accurate keeping of accounts and records 36
5.3 Appendix 3; Whistleblower policy 37
5.3.1 Introduction 37
5.3.2 Notification procedure 37
5.3.2.1 When should you report an issue? 37
5.3.2.2 You must proceed responsibly when making a notification 38
5.3.2.3 How should the company react when notified 39
5.3.2.4 Prohibition against retaliation 39
5.4 Appendix 4; Gifts and Business Hospitality Procedure 41
5.4.1 Introduction 41
5.4.2 General checklist 41
5.4.3 Limits for self-approval and further guidance 42
5.4.3.1 Gifts 42
5.4.3.2 Meals 42
5.4.3.3 Travel 43
5.4.3.4 Entertainment 43
5.4.4 Control measures 43
5.5 Appendix 5; Integrity Due Diligence Procedure 44
5.5.1 Introduction 44
5.5.2 Integrity due diligence 44
5.5.2.1 Initial red flag assessment 44
5.5.2.2 Situations in which a background check is not required 45

5.5.2.3 Implementation of background checks 46
5.5.2.4 The result of the background check 46
5.5.3 Measures to mitigate risk 47
5.5.4 Privacy in connection with background checks 47
5.6 Appendix 6; Sanctions Compliance Policy 54
5.6.1 Introduction 54
5.6.2 Legal framework 54
5.6.3 Company policy 55
5.6.4 Responsibility 56
5.7 Appendix 7; Cyber Security Policy 58
5.7.1 Introduction 58
5.7.2 Checklist 59
5.8 Appendix 8; Data Protection Policy 62
5.8.1 Objective 62
5.8.2 Regulatory requirements 62
5.8.2.1 Territorial scope 62
5.8.2.2 Material scope 63
5.8.3 Data protection principles 64
5.8.3.1 General 64
5.8.3.2 The principles 64
5.8.4 Legal basis 66
5.8.4.1 General 66
5.8.4.2 Regular personal data 66
5.8.4.3 Special categories of data (sensitive data) 68
5.8.4.4 Consents 69
5.8.4.5 Criminal offences and convictions 69
5.8.4.6 Unique identifiers 69
5.8.5 Transparency 70
5.8.5.1 General 70
5.8.5.2 Content of the privacy information 70
5.8.5.3 Communication of the privacy information 70
5.8.5.4 Data subject rights 70
5.8.5.5 Automated decision-making 70
5.8.5.6 Marketing 70
5.8.5.7 Privacy by design and privacy by default 71
5.8.5.8 Joint control 71
5.8.6 Transfer to countries outside the EU/EEA 71
5.8.7 Processors and DPAS 71
5.8.7.1 General 71
5.8.8 Data sharing with independent controllers 72
5.8.9 Records of processing activities 73
5.8.10 Data security 73
5.8.11 Data breach handling 74
5.8.12 Privacy risk assessment 74
5.8.13 Data protection impact assessment 74
5.8.14 Identifying lead supervisory authority 75
5.8.15 Training 75
5.9 Appendix 9; Personal Trading Policy 76
5.9.1 Purpose 76
5.9.2 Personal transactions 76
5.9.2.1 Introduction 76

5.9.2.2 Limitations, exceptions and discretionary exemptions 76
5.9.2.3 [Optional: Existing investments in violation of the regulations 77
5.9.2.4 General checklist 77
5.10 Appendix 10; Payment Procedure 78
5.10.1 Introduction 78
5.10.2 Control environment 78
5.10.3 Checklist – payment execution 80
5.10.3.1 Chart of Accounts - Online Bank 80
5.10.3.2 Approval Matrix – Online Bank 81

2 Responsibility

Managers of the business areas and legal entities in EUREKA GROUP are responsible for the contents and requirements of this document being known, implemented and complied with in the individual unit(s). The term "employee" used in this document denotes permanent employees, temporary employees, and hired consultants.

In the event of any cases of discrepancy between current legislation and EUREKA GROUP's governing documentation, current legislation is always to apply – that is if not the internal rules are stricter.

3 Values

EUREKA GROUP has defined four core values that help form the basis of a good reputation, important for EUREKA GROUP to be able to realize its business ambitions. EUREKA GROUP's reputation takes long to build up, but it may take a short time to destroy it.

As employees of EUREKA GROUP we are all responsible for maintaining and building a good reputation. This reputation is primarily developed through the attitudes and conduct of the individual employee. We shall never set aside our values in order to obtain financial benefits.

EUREKA GROUP's core values - **PACE**:

- "**PROFESSIONAL**"; this describes the quality of our supplies. Our work is well structured, we have an appropriate conduct, we deliver as promised and at the right time, and we charge a correct price for the job.
- "**AMBITIOUS**"; this suggests that we are determined and self-respecting. We set high goals because we want to achieve a lot. We strive to reach further, we are on the alert, we always do a little extra.
- "**CARING**"; embraces the way we deal with each other. It says that we care about each other. We make each other good, we look after each other, we see each other, and show consideration, we wish each other well.
- "**ENTHUSIASTIC**", is contagious! "Enthusiastic" embraces job satisfaction, positivity, high spirits and energy. We thrive in our good working environment – and we show it.

4 Code of Conduct

4.1 General

Ethics has to do with the individual's conscience, i.e. distinguishing right from wrong. Ethical awareness cannot be adopted. Ethics, and a wish to act ethically, must spring from a basic desire to act in an honest, decent and orderly manner.

By way of EUREKA GROUP's Code of Conduct, management puts words to the basic values that we require all employees of the group to support through behaving responsibly in relation to colleagues, customers, partners, and the community at large.

EUREKA GROUP's Code of Conduct is based on the following main elements:

- We act in an honest, decent and orderly manner
- We shall comply with all acts and regulations in effect for the work
- We shall not abuse our position to obtain personal gains for ourselves or others
- We do not participate in corrupt and unacceptable business transactions
- We do not participate in acts whose purpose is to harm people or assets

4.2 Business Ethics

EUREKA GROUP's business operations include a wide range of activities, values and interests. Taking part in these activities gives the employee stimulating challenges and possibilities for personal development. However, such participation also poses demands on individual conduct and responsibility.

At times, we may become exposed to inappropriate pressure or be tempted to put personal gain above the interests of EUREKA GROUP. EUREKA GROUP can also be afflicted damage or loss inadvertently due to ignorance or carelessness.

EUREKA GROUP sets absolute standards for employee honesty and integrity in all matters having to do with the group. Our operations must abide by the same ethical requirements no matter where in the world we are operating. All employees must ensure that operations comply with current laws and regulations that apply at the locations where the group is represented and carry out their work in accordance with the requirements laid down in this document. In this way we contribute to exercising corporate social responsibility securing EUREKA GROUP's good reputation, and reducing risk, both for the group and the individual.

EUREKA GROUP base operations on 10 principles which are described in appendix 1.

These 10 principles are;

1. We comply with laws
2. We respect our colleagues

3. We ensure healthy and safe working conditions
4. We protect our assets and confidential information
5. We respect fundamental human rights
6. We never make illegal payments
7. We select our business partners carefully
8. We avoid conflicts of interest
9. We compete fairly
10. We operate in an environmentally responsible manner

This means all employees must:

- abide by all EUREKA GROUP principles and overall requirement documents for business activity, and always act in the interest of EUREKA GROUP,
- actively advocate and pursue honesty and integrity in all business activities,
- refrain from divulging or abusing confidential information,
- act impartially in all business matters and refrain from giving any undue advantages to business connections,
- employ facts and existing contracts / agreements as basis for resolving disputes and disagreements,
- avoid engaging in matters that may conflict with EUREKA GROUP's interests, or which may in any way negatively affect one's freedom of action or independent judgement,
- in connection with any direct or indirect gift, token of recognition, travel, service or other benefit, unless this were to be of negligible value (+/- NOK 500.-), inform and apply for the approval of the employee's superior. Similar rules apply regarding gifts, recognitions etc., which are offered by business areas/employees of EUREKA GROUP to external business connections. The individual employee is responsible for raising issues of concern and asking his/her nearest superior in cases of doubt or where there is room for interpretation.

4.3 Own behavior

EUREKA GROUP expects employees to have a correct conduct and to treat everyone they get in contact with through work or work-related activities with courtesy and respect. This includes being aware of and respecting different cultures and customs, and actively promoting a working environment characterized by equality and diversity. EUREKA GROUP employees are responsible for protecting the group's reputation and for acting in accordance with expectations held out by the group.

Employees are expected to contribute to an orderly and effective work environment. Employees must therefore perform their work to their utmost ability and refrain from any conduct which might have a negative effect on colleagues or the work

environment. The principles of not discriminating and showing tolerance and respect for one's colleagues must likewise support and characterize all conduct displayed.

EUREKA GROUP does not accept any kind of discrimination or harassment of own employees or others involved in the EUREKA GROUP's activities. Discrimination includes all differential treatment, exclusion, or preferences based on gender, race, age, functional ability, sexual orientation, religion, political views, nationality, ethnic background or similar, which leads to the principle of equality being neglected.

Employees have a duty to inform the EUREKA GROUP CEO and/or Chairman of the Board of EUREKA GROUP AS if, directly or indirectly, by consanguinity or other close relationships, they have a material interest in an agreement entered by an EUREKA GROUP company.

4.4 Directorships and other work-related matters

EUREKA GROUP is generally positive to employees' taking on duties in other undertakings. However, employees cannot take on such commissions in companies that are competitors to EUREKA GROUP. All such commissions must be approved by the closest superior and general manager of the company. As concerns general manger, he/she will acquire such approval from the CEO of EUREKA GROUP.

EUREKA GROUP employees shall not have paid work outside of EUREKA GROUP, except as expressly agreed with the company.

Should conflict of interest arise in any way, or the employee's ability to perform his/her work and obligations towards EUREKA GROUP cannot be complied with, such approval shall not be granted, or be revoked.

4.5 Information and IT systems

Information produced and stored on EUREKA GROUP's system(s), is regarded as EUREKA GROUP property. EUREKA GROUP therefore reserves the right of access to all such information, unless such right is limited by laws or agreements. All employees are responsible for keeping electronic files and archives tidy.

Use of information, the IT system and especially Internet services, must be exercised based on business needs, not personal interest. Also, information of a personal nature must not be downloaded or stored on EUREKA GROUP's systems. Use of software in violation of copyright provisions, is prohibited.

EUREKA GROUP has established a separate requirement document related to "Information technology", EPS-MGM-0010 Information Technology Management, giving more detailed requirements related to use of EUREKA GROUP IT systems.

4.6 Confidentiality

It will be natural for employees to talk about their work and company activities with colleagues, family or friends. In general, this is not a problem, although some categories of information are strictly controlled and must not be disclosed to anyone without a need for and right to gain knowledge of the information. Such information must only be publicized internally or externally by personnel authorized to do so.

Employees must also consider where and when to talk about EUREKA GROUP-related matters to ensure that unauthorized personnel do not gain access to the information. As an employee you have an obligation to maintain professional secrecy in relation to unauthorized persons about matters that you learn about through your work in EUREKA GROUP, including information received from customers and partners, and to treat such information with care, also in relation to other employees in EUREKA GROUP.

Employees must treat as confidential all information classified as ”Confidential” or which for the following reasons must not be made known to unauthorized personnel: security, protection of privacy, sensitivity, business integrity, commercial or technical advantages/leads, contractual relationships or in accordance with acts. The employee undertakes to observe confidentiality also after cessation of his/her employment with EUREKA GROUP.

These guidelines are described in appendices 7 and 8.

4.7 Bribes and corruption

Corruption undermines legitimate business activity, distorts competition, ruins reputations and exposes the company and individuals to risk. From time to time, EUREKA GROUP employees may get into contact with corrupt activities.

EUREKA GROUP will not take part in any corrupt activities, and neither will it accept any offers, payments, demands for or receiving of bribes in connection with its business activity. Any case of corruption or bribe, or attempted corruption or bribe, must be reported to the group management immediately.

“Facilitation payments”

” Facilitation payments” are here defined as payment of a small amount to a public servant, where the sole intention is to speed up a routine administrative process he has a duty to perform and where the outcome is predetermined. This means the payment is not intended to affect the outcome of the official action, merely time spent in the process. It is not uncommon for public officials in some countries to refuse to perform the work they have been assigned to, unless they receive money for it (in some cases, such payment claims have almost been put into system as remuneration of public servants).

EUREKA GROUP's attitude is that we must refrain from making facilitation payments. There are no exceptions. In doubt, i.e. if omitting use of minor facilitation payments will have large negative consequences on personnel, assets or customer deliveries, the employee should contact his/her manager for advice.

These guidelines are described in appendix 2.

4.8 Whistleblowing

Blowing the whistle is to report blameworthy conditions in the workplace.

A good working environment has a low threshold for exposing blameworthy conditions. Criticism and disagreement are handled in an impartial and orderly manner. Transparency in the workplace shows a healthy corporate culture, with which both EUREKA GROUP and employees are served. As an employee you have the right, and in some cases also the duty, to expose blameworthy conditions in the workplace.

Examples of matters that it may be relevant to report:

- Failure of safety procedures
- Working conditions in violation of requirements in the Working Environment Act
- Conditions in violation of EUREKA GROUP's steering documentation
- Irresponsible procedures
- Corruption or other financial fraud

When/if you discover conditions in the workplace that you react to, you must carefully consider whether you are to report the matter, or whether your procedure for reporting it is appropriate.

The following possibilities for whistleblowing have been established:

- Using the electronic" whistleblowing procedures" in the companies' management systems and or/Intranet
- Contacting your superior of another EUREKA GROUP supervisor in whom you have confidence
- Submitting a written or oral report to the chairman of the board or one of the directors of EUREKA GROUP AS' board

If desirable, all whistleblowing will be treated anonymously.

These guidelines are described in appendix 3.

4.9 Implementation

In addition to this document, EPS-MGM-0009 Authorizations, which defines the authorization matrix for EUREKA GROUP and its subsidiaries, should be communicated to the employees;

- Group management should review EPS-MGM-0008, Values and Ethics' and EPS-MGM-0009, Authorizations a minimum of once a year.
- Each business area should at least once a year discuss EPS-MGM-0008 and EPS-MGM-0009 Authorizations in a senior management meeting
- Each business area should at least once per year give highlights from EPS-MGM-0008 and EPS-MGM-0009 Authorizations in a 'Allmøte'
- All employees should sign that the EPS-MGM-0008 is read and understood

4.10 Consequences of violation

Violation of the EUREKA GROUPS's Code of Conduct or applicable laws may lead to disciplinary action or cause charges to be brought to the relevant authorities. Employees, who offer, pay, demand or accept bribes may become dismissed from their job and brought to face charges.

Company procedures will be detailed when it comes to disciplinary action by the company.

4.11 Guidelines for Sanctions of Compliance

We have a policy of strict compliance with all applicable laws in relation to trade sanctions and anti-terrorism.

This policy describes the legal framework and company policy in relation to trade sanctions and regulations governing the cross-border movement of products, funds, technology and services.

These guidelines describe the legal framework and EUREKA GROUP's policy with respect to trade sanctions and rules that are related to movement of goods, financial assets, technology, and services across borders.

These guidelines are described in appendix 6.

4.12 Guidelines for Integrity Due diligence

A key principle in our Code of Conduct is that we should select our business partners carefully. Our IDD efforts should be risk-based, meaning that we will not apply the same process to all business partners. The level of due diligence will be determined based on the application of a step-by-step approach described in this procedure.

The term 'business partners' should be taken to mean all entities or individuals with which our company enters into a business relationship, and includes suppliers, consultants, agents, joint venture partners, lobbyists and other intermediaries.

5 Appendices

Appendix 1; Guidelines for Code of Conduct

Appendix 2; Anti-Corruption Policy

Appendix 3; Whistleblower policy

Appendix 4; Gifts and Business Hospitality Procedure

Appendix 5; Integrity Due Diligence Procedure

Appendix 6; Sanctions Compliance Policy

Appendix 7; Cyber Security Policy

Appendix 8; Data Protection Policy

Appendix 9; Personal Trading Policy

Appendix 10; Payment Procedure

5.1 Appendix 1; Guidelines for Code of Conduct

CONFIRMATION FROM EMPLOYEE

Confirmation of compliance form

A culture of compliance is fundamental to protect our company values and our reputation in the market. Compliance is about operating within the legal framework of the countries in which we operate. Our objective is complete and absolute compliance. By allowing minor deviations or exceptions we legitimate more serious violations of the laws. Consequently, we do not distinguish between important laws and less important laws.

On behalf of EUREKA GROUP, we hereby request your kind confirmation of your compliance with applicable internal guidelines of EUREKA GROUP when acting on behalf of the company or any of its subsidiaries or affiliates.

We request you to fill in the details below, including your signature. Please return signed form to the HR department.

I hereby confirm that I have received a copy of the EUREKA GROUP guidelines for Values & Ethics (EPS-MGM-0008), including the appendices;

Appendix 1; Guidelines for Code of Conduct

Appendix 2; Anti-Corruption Policy

Appendix 3; Whistleblower policy

Appendix 4; Gifts and Business Hospitality Procedure

Appendix 5; Integrity Due Diligence Procedure

Appendix 6; Sanctions Compliance Policy

Appendix 7; Cyber Security Policy

Appendix 8; Data Protection Policy

Appendix 9; Personal Trading Policy

Appendix 10; Payment Procedure

I hereby confirm that I, to the best of my knowledge, have complied with and will continue to ensure compliance with, the aforementioned documents in every respect when acting on behalf of EUREKA GROUP.

Name:

Position:

Date:

Signature:

This Code of Conduct applies to all employees. It also applies to board members, owner representatives, independent contractors and consultants, temporary employees and hired employees. Every time we engage someone to perform services on our behalf, we will request the service provider, agent or consultant to comply with our Code of Conduct. Alternatively, they should demonstrate that they are bound by other ethical guidelines demonstrating similar expectations regarding ethical, responsible and profitable decisions.

The ten principles included in this Code of Conduct are:

1. **We comply with laws**
2. **We respect our colleagues**
3. **We ensure healthy and safe working conditions**
4. **We protect our assets and confidential information**
5. **We respect fundamental human rights**
6. **We never make unlawful payments**
7. **We choose our business partners carefully**
8. **We avoid conflicts of interest**
9. **We compete fairly**
10. **We operate in an environmentally responsible manner**

If you are ever in doubt as to whether a decision is in line with the principles set out in this Code of Conduct, do not hesitate to ask or seek advice. You first point of contact should always your line manager. The management recognizes that most employees will face ethical dilemmas during their employment. We encourage you to address these dilemmas openly. Open and honest discussions are necessary to ensure that we are all on the same track.

To safeguard the company's interests, we expect you to notify us if you observe someone acting in violation of the Code of Conduct. Talk to your supervisor or use the channels of notification described in our Whistleblower Policy if you have any concerns. You will never experience negative reactions from the company if you alert us of an issue properly and in good faith.

You are expected to read the Code and confirm in writing that you will comply with it. If you have any questions about the Code and its, please do not hesitate to ask your line manager. Take your time studying this Code of Conduct.

5.1.1 Principle 1: We comply with the law

A culture that expects compliance with laws and regulations is of fundamental importance to safeguard the company's values and our reputation in the marketplace. It is about operating within the legal framework in the countries where we operate. Our goal is to be fully compliant. If we allow small deviations or exceptions, this may legitimize violations that are more serious. Consequently, we do not distinguish between important and less important laws.

The term "laws" shall be understood as acts, regulations and injunctions at national and local level. Furthermore, we expect you to comply with our internal policies and procedures. This Code of Conduct is intended to help us comply with the law, fulfil important goals for the company and make our teamwork easier. Such "company rules" must be studied and complied with.

Compliance requires commitment. We expect you to seek guidance and to seek legal advice if you are ever uncertain about the legality of your actions. You shall not operate in "grey areas" and expose yourself and the company to unnecessary risk.

Compliance with the regulations is a joint responsibility. To reach the goal of this Code of Conduct, there are certain legal obligations that are especially important:

- ⇨ To comply with laws and regulations relating to the safety of our employees;
- ⇨ To comply with laws and regulations that protect the environment;
- ⇨ To comply with accounting standards and laws aimed at ensuring the accurate keeping of accounts and records;
- ⇨ To comply with laws relating to calculation and deductions of taxes and public duties;
- ⇨ To comply with laws in connection with the working environment;
- ⇨ To comply with laws that ensure fair competition and prohibits unlawful business activities such as corruption and fraud;
- ⇨ To comply with laws that for foreign policy and security reasons prohibit trade and business with certain countries, organizations and individuals;
- ⇨ To comply with laws, rules and regulations relating to the fight against money laundering;
- ⇨ To comply with the data protection legislation that applies to our operations.

In certain areas, such as sanctions and export control, the company may have adopted stricter policies than required by national laws. The reason may be that we operate in several countries and therefore have decided to abide by laws other than the ones applicable in our home country. When there is a difference in standard between the requirements established by law and the requirements of our internal guidelines, the highest standard shall apply.

5.1.2 Principle 2: We respect our colleagues

Our goal is to recruit, develop and retain the best employees, and we want a creative, diverse and including working environment.

We want our employees to reach their full potential and be recognized and rewarded for their performance in a fair manner. To help you achieve and perform according to your full potential, colleagues may provide honest feedback in a constructive and respectful manner. The management encourages input from the company's employees.

We have zero tolerance for harassment, discrimination and bullying based on race, gender, age, nationality or social background, disability, sexual orientation, religious faith and political beliefs. We should treat everyone politely and with respect, and we should never tolerate any form of violation of our colleagues, contractors, suppliers, customers or anyone with whom we trade.

We believe everyone should have equal opportunities. Therefore, we will recruit, select, train, promote and reward our employees based on results and fair criteria. All decisions should be based on qualifications, demonstrated capability, performance or other professional criteria.

We also expect our contractors, suppliers, customers and other business partners to aspire to similar standards of fair treatment and equal opportunities for their employees. The term "contractor" shall be understood to mean both those who work in our organization as hired personnel and those who work for a supplier or service provider.

You should never:

- ⇨ Act in a manner that may be reasonably be considered insulting, threatening, discriminatory or offensive. That means, among other things, avoiding offensive language or inappropriate jokes, of e.g. a racial or a sexual nature, in the workplace;
- ⇨ Engage in any form of harassment. Harassment does not have to take place at work or affect a colleague to violate our policies;
- ⇨ Humiliate, ridicule or hurt another person;
- ⇨ Directly or indirectly discriminate against an employee based on race, gender, age, national or social background, disability, sexual orientation, religious faith or political beliefs;
- ⇨ Pretend not to notice harassment or discrimination in the workplace. Raising concerns or reporting incidents to the management will never result in retaliation.

For further guidance, please see:

- Our Employee Handbook
- Our HR Policy
- Our whistle blowing policy

5.1.3 Principle 3: We ensure healthy and safe working conditions

We aim for a healthy workforce and a safe working environment, and we are committed to safeguarding the health and well-being of all our employees.

The company will always comply with applicable law and regulations related to health and safety in the workplace. You must study and follow management guidelines and instructions, as well as policies and procedures that apply to your area of work. You must be helpful and cooperative towards those who are responsible for ensuring that health and safety requirements are met.

In certain projects, we may also be required to comply with instructions from other companies, such as the customer or the operating company. It is important to always comply with such instructions, and you must be aware that failure to comply may have serious economic consequences for the company, in addition it may result in personal injury or material damage if something goes wrong.

Health and safety issues, work-related injury or illness must be reported immediately. Employees who become aware of a potentially dangerous situation or a near accident should also report this without delay. You may always report such concerns to your line manager or by following the procedure in the company's whistleblower policy.

Being under the influence of alcohol or drugs, or abusing medications, clouds our judgment and our performance at work and will not be tolerated in the workplace. It may compromise both your own and your colleagues' safety.

Only accept work that you are qualified for and that you are in adequate shape to, prepared for and rested enough to perform. You should always take the time to plan and perform the work properly. You must ensure that everyone involved in the work fully understands all the aspects of our activities, as well as any other activities that take place concurrently and that may potentially affect our activities.

As employer, we will ensure that:

- ⇨ We comply with all laws and regulations relating to the safety of our employees;
- ⇨ The working conditions in the company meet or surpass international standards of work, including the conventions and recommendations of the International Labor Organization;
- ⇨ The workplace, machinery, equipment and procedures are safe and without risk to the employees' health;
- ⇨ Suitable protective measures are always taken.

You must always use the protective gear and clothing provided by the company, as this is provided to prevent the risk of accidents or adverse health effects. You are required to study the requirements for use of protective equipment and protective clothing for the various operations in which you participate.

You are required to be careful about your own health and safety. You have an absolute duty to stop any work you believe to be unsafe.

5.1.4 Principle 4: We protect our assets and confidential information

We are always careful to protect our business assets and confidential information. Such assets and such information include property, intellectual property, business opportunities, customer lists, pricing and other issues concerning the company's funds and equipment. We also respect the intellectual property and trade secrets of others.

As a company, we are committed to the proper administration of our accounts and to meeting the requirements of financial laws and regulations. We are required to disclose the company's operations openly and accurately, and to submit financial reports or other statutory public reports.

We also protect access to and proper use of the company's information and IT resources.

We are all responsible for ensuring that our assets are not abused or destroyed. Examples of abuse are theft of supplies, equipment, documents, cash or other property.

Ensure that you:

- ⇨ Exercise reasonable care always when using our property, ensuring that it is not damaged or lost;
- ⇨ Immediately report lost or stolen property and / or equipment;
- ⇨ Treat the company's funds as you would have treated your own funds and do not abuse telephones, computers or other equipment;
- ⇨ Do not use company property for personal activities without prior approval;
- ⇨ Protect company information and never disclose confidential or internal information to non-employees. This obligation does not only apply during your employment, but also after your employment has ended;
- ⇨ Talk to your supervisor if you suspect that confidential information has been abused or disclosed to others.

Employees and their family members must not buy or sell shares or other securities, or provide advice related to trading in securities, while in possession of inside information that they may acquire during the course of their employment, and which relates to the shares of any customer, supplier, transaction counterpart or partner of the Company.

"Inside information" is information which may noticeably affect the price of any listed company or listed financial instruments. If you have any doubt as to whether you possess inside information, you should contact your immediate superior or the Company's representative in charge of insider trading matters, and the advice of legal counsel may be sought.

All Employees of the Company must exercise caution not to disclose inside information to outsiders, including colleagues, unless clarified with the company representative in charge. The term "disclose" covers intentionally or inadvertently acts, under any circumstances, whether at meetings held as part of the business day or elsewhere. The Managing Director or someone authorised to make statements on behalf of the company shall coordinate any media contact. You are not allowed to make statements to the press on issues that apply to the company without prior approval.

5.1.5 Principle 5: We respect fundamental human rights

We will protect the fundamental human rights of everyone affected by our activities. This is especially important when we operate in areas and regions with low standards of living and poor protection of human rights by the national authorities. We recognize that respect for human rights is a global standard and that our responsibility to respect and comply with human rights applies to all activities wherever we operate. This standard takes precedence over national laws and is intended to ensure that fundamental rights are protected when local law and standards do not provide adequate protection.

We will respect human rights in accordance with the UN's guiding principles. As a company, we support the principles of the UN Global Compact (UNGC), which means that we will work actively to integrate human rights into our practices and business activities, as well as continuously try to uncover the risk of violations in connection with our activities. We shall:

- ⇨ Avoid creating or contributing to human rights violations through our operations. We will demand that our contractors and suppliers also respect human rights in accordance with the UN's guiding principles;
- ⇨ Work actively against negative impact on human rights when they occur;
- ⇨ Seek to prevent or minimize human rights violations directly related to our activities, products or services;
- ⇨ Never use child labor or forced labor in our own operations, and commit our contractors and suppliers to do the same;
- ⇨ Recognize the right to collective bargaining and the freedom of association;
- ⇨ Provide all our employees with a decent salary and regulated working hours;
- ⇨ Respect the cultures of indigenous people and recognize their right to practice their traditions and customs.

Human rights are defined by conventions and principles, such as the UN's international conventions and declarations on human rights and ILO's core labor standards conventions. This includes, but is not limited to, human rights such as those set out in UN International Covenant on Civil and Political Rights (1966), UN International Covenant on Economic, Social and Cultural Rights (1966), UN Convention on the Rights of the Child (1989), UN Convention on the Elimination of All Forms of Discrimination against Women (1979), the ILO Minimum Age Convention (no. 138) and ILOs fundamental conventions on rights at work. Further, by expressing our support to UNGC, we are dedicated to supporting ten internationally recognized principles in the areas of human rights, labor standards, environmental sustainability, and anti-corruption. *[If the company has already signed UNGC, this text must be adjusted.].* We expect you to study the ten principles of the UN Global Compact (www.unglobalcompact.org).

We understand that protection of human rights is not only the responsibility of the government, but that we have an independent responsibility to safeguard human rights through our activities.

Our goal is to make a positive contribution to the societies in which we operate by safeguarding human rights by developing businesses, encouraging innovation and increasing international competitive power.

To that end, we will ensure compliance with the requirements set out in the Norwegian Transparency Act, including but not limited to the requirements set out in respect of due diligence assessments to be undertaken in that regard.

For further guidance related to human rights and the due diligence assessment to be undertaken in that respect, see our:

- Due Diligence assessment procedure (appendix 11)

5.1.6 Principle 6: We never make unlawful payments

Unlawful payments include all types of payment that is unlawful under applicable law. The term "unlawful payments" includes corruption, misappropriation and fraud. An unlawful payment will typically result in the enrichment of one or several individuals at the expense of the company and will usually be contrary to the company's interests. Any business advantages to our company will nevertheless never be an extenuating circumstance in the event of an unlawful payment. Such payments are strictly prohibited and will in most cases result in the immediate termination of your employment.

Unlawful payments constitute a threat to fair competition and undermine legitimate business activities. Any violation by one of our employees constitutes a threat to our reputation and our credibility in the market.

It is not permitted to give, offer, accept or receive an improper advantage to or from a person in the public or the private sector by virtue of one's position. In addition to money, gifts, services, offers of favorable terms and conditions for a product or a service, as well as travel and subsistence, may constitute an improper advantage and consequently be a violation of the rules of corruption.

Our policy is to comply with the Norwegian anti-corruption provisions, the UK Bribery Act, UKBA, the US Foreign Corrupt Practices Act, FCPA as well as any other applicable law.

Furthermore, it is strictly prohibited to make an unauthorized transfer of money or something else of value from the company to yourself, to any of your close relatives or another person that acts on your behalf.

For anti-corruption guidance, please see our:

- Anti-corruption Policy (appendix 2)
- Gifts and hospitality procedure (appendix 4)

5.1.7 Principle 7: We carefully choose our business partners

Our business partners are important to our company's success, and we aspire to build good and lasting relationships with our partners. The term "business partners" includes our suppliers, contractors, joint venture partners, agents, customers, consultants, professional advisors, etc. *[Please change the list based on the company's profile]* Our company will be identified with our business partners and their conduct may therefore affect the company's reputation and expose us to other negative consequences. For this reason, we must choose our business partners carefully, particularly when the business partners provide services on our behalf.

The due diligence a new business partner requires will depend on the risk factors or "red flags" that are present. We expect you to:

- ⇨ Investigate whether the business partner's home country is at high risk of corruption (see Transparency International Corruption Perceptions Index);
- ⇨ Perform a risk-based background check as prescribed in the company's IDD procedure. You must never cooperate with a business partner without conducting an initial assessment of the company's reputation and obtaining certain key information about the relevant company;
- ⇨ Use contract clauses to commit business partners to adhere to our standards in relation to anti-corruption, working conditions as well as the environment and human rights;
- ⇨ Monitor our business partners' performance and act immediately if a business partner fails to fulfil their contractual obligations, or if you suspect unlawful activities;
- ⇨ Be aware of the risk of receiving or handling the proceeds from a criminal offence (money laundering). You must always know who the business partner is, obtain confirmation that transfers are being made to and from the correct bank accounts, and be on the lookout for red flags in a specific transaction;
- ⇨ Study applicable laws relating to trade restrictions and counter terrorism measures, and ensure that you do not become involved with companies or individuals subject to sanctions;
- ⇨ Ask yourself if an agreement seems to be in accordance with market practices and commercially acceptable terms and conditions. The fee and the price must be defensible and proportionate to the goods or services provided
- ⇨ Be aware of the possibility of false invoices, false agreements or unidentified costs on invoices payable by the company.

The use of agents or intermediaries to obtain or retain business opportunities or to obtain certain permits from government agencies may sometimes expose the company to an unacceptable level of risk. You must never engage an agent or an intermediary to assist in business development or to achieve a result in respect of public authorities without the prior approval of the Managing Director.

For further guidance, see our:

- IDD procedure (appendix 5)

5.1.8 Principle 8: We avoid conflicts of interest

Conflicts of interest arise when our personal, social, financial or political activities affect the work we do or our loyalty to the company. We expect you to always act in the best interest of the company, and not make decisions based on what will benefit you personally. Nor should you use confidential company information you receive as an employee of the company for personal or others' gain.

When possible, conflicts of interest should be avoided. Sometimes, just the fact that something *seems* to be a conflict of interest may be detrimental to the company. If a potential conflict of interest arises, it is important that you acknowledge it, disclose it to your supervisor and ask for appropriate guidance.

Sometimes, conflicts of interest may be difficult to identify. You should ask yourself if the situation affects how you do your job or if it affects decisions you make on behalf of the company. You also must consider what the situation looks like from the outside. Will your colleagues or the company's shareholders, contractors or customers think that the situation could affect the performance of the job you do for the company?

Please be aware that the following situations may create an actual or an apparent conflict of interest:

- ⇨ If you have another job or perform services on behalf of one or more of our competitors, customers or suppliers;
- ⇨ If you operate a business in your own time that is similar to your work in the company;
- ⇨ If you have a personal or financial interest in a business that has transactions or business with the company, such as one of our competitors, customers or suppliers;
- ⇨ If one of your family members or another person with whom you have a close personal relationship, have business with the company;
- ⇨ If you or any of your family members or another person with whom you have a close personal relationship, invest in one of the company's competitors, suppliers or customers.

You should always disclose any actual or potential conflicts of interest to your supervisor.

5.1.9 Principle 9: We compete fairly

We support open and fair competition in all markets.

We are committed to comply with all competition laws or antitrust laws that prohibit conduct that restricts trade or prevents competition. We will not pursue anti-competitive practices. Anti-competitive practices include agreements with a competitor to fix or align prices, share or allocate markets, rig tenders or limit or restrict supply to customers. Such practices may also include agreements that impose restrictions on customers and suppliers.

The exchange of information may also be anti-competitive. Therefore, you should never share competitively sensitive information with a competitor, such as information on present and future prices, costs, strategies, customers or suppliers. To receive such information from a competitor is also unlawful. This prohibition also applies when we participate in industry organizations or joint ventures with competitors.

You should never agree or signal that you are willing to:

- ⇨ Conclude agreements with a competitor on; (i) prices for a third party, (ii) the time of a price increase or price reduction, or (iii) other pricing conditions;
- ⇨ Split certain customers, territories or markets with a competitor;
- ⇨ Discuss competing offers or tenders with a competitor, or agree who should win a tender;
- ⇨ Agree with a customer on which price the customer may charge to its customers, or agree on a minimum price for resale;
- ⇨ Instruct a customer only to purchase from the company, or require a supplier to only sell to the company;
- ⇨ Restrict in which area or to whom a customer may sell, or in which territories the customer may sell;
- ⇨ Conduct that abuses a position of market dominance.

Competition law violations are subject to strict penalties, and allegations of anti-competitive practices may damage the company's reputation. Seek advice in any situation that you think may involve a risk of competition law violations, and report to the management if there is a risk that the company may be exposed.

5.1.10 Principle 10: We operate in an environmentally responsible manner

We are all responsible for protecting the environment. As a company, we want to comply with all legislation and regulations relating to environmental protection.

We are committed to ensuring that the environmental impact of our operations is reduced wherever possible. This includes, but is not limited to, reducing the impact on local biodiversity, reducing emissions (including greenhouse gases) and waste to the minimum possible and handle, move, store, use, recycle and reuse hazardous substances, chemicals, waste, or similar materials in a safe manner.

We will monitor and assess negative environmental impacts of our operations and will always address these and seek to improve them. We are committed to striving for best industry practice whenever possible. We will seek to ensure efficient use of natural resources and will consider the environmental impact when choosing a product or a work procedure for a project in which we are involved. Environmental considerations shall be an integral part of the assessment in all procurement and when choosing suppliers.

All employees are expected to comply with our environmental protection procedures.

You must report all incidents that occur and that may affect the environment.

You must also report all apparent environmental law violations to the management.

5.2 Appendix 2; Anti-Corruption Policy

5.2.1 What is corruption?

Corruption is abuse of a position of authority for personal gain. It may take the shape of bribes, trading in influence and palm greasing. Our company and our employees are subject to a variety of anti-corruption laws from many parts of the world. We will comply with applicable anti-corruption law in the countries in which we operate. This includes, among others, the Norwegian statutory provisions on corruption, the UK Bribery Act (UKBA) and the US Foreign Corrupt Practices Act (FCPA).

Based on this, you are prohibited from:

- Providing or offering an improper advantage by virtue of your position, office or engagement in the public or the private sector;
- Offering, promising or giving an economic or other type of advantage to another individual for the purpose of (i) inducing the individual to perform a relevant function or activity in an improper manner, or (ii) rewarding an individual for improper performance of such function or activity;
- Offering to pay, pay or allow payment of money or something else of value to a foreign civil servant for the purpose of influencing an act or decision of the civil servant in his/her official capacity. The same applies to the securing of other improper advantages for the purpose of obtaining or retaining business opportunities;
- Falsifying the company's accounts and records;
- Paying so-called "facilitation payments";
- Offering or giving an improper advantage to a third party in exchange for this individual trying to influence the conduct of somebody else (trading in influence).

5.2.2 Bribes

Giving and receiving a bribe is prohibited. It is enough *to make an offer* to be held liable under applicable anti-corruption law. No actual transfer needs to be performed.

Anti-corruption laws apply to both the public- and the private sector. Your personal opinion about the intent behind your actions will not carry weight, as the prosecuting authority will evaluate the circumstances objectively.

The following are typical characteristics of a corrupt payment:

- Personal enrichment of decision-makers (in the public or the private sector) or anyone in your company;
- It is not given or offered openly;
- Measures are taken to conceal or disguise the cash flows.
- It is paid for the purpose of influencing a decision of significance, for example; a tender, contractual negotiations, a public sector permit or licence, or the participation in a joint venture.

Example 1 – "Kickbacks"

A Purchasing Manager in an oil service company is offered to have 2% of the value of a software contract paid to him personally if he can "deliver the contract". The contract is related to the new software, and there are several potential suppliers. Instead of transferring the money directly, the Purchasing Manager and the software company agree to set up false contracts and false invoices from the Purchasing Manager's private investment company to make it look like a normal trade.

Legal implications: The Purchasing Manager and the software company may be criminally liable pursuant to applicable anti-corruption law.

It is not only the transfer of money that may constitute corruption. In addition, gifts, loans, services and offers of favorable terms for a product or a service, travel, accommodation, entertainment and donations to charitable organizations for improper reasons may constitute bribes.

Whether an advantage will be considered "improper" by the prosecuting authority or the court depends the monetary value, the roles of the parties involved the frequency and extent of activity and the reason for offering the advantage.

For example, it may be acceptable to give a gift to the Managing Director of a joint venture partner on the tenth anniversary of a project at a joint event. However, it would probably not be acceptable to give the same gift in secret during the contract negotiations to try to influence the joint venture agreement for the advantage of their own company.

Dilemma 1 – Services

Your company uses a carpenter for renovation work in the office building. He is good at his job and reliable. When you are planning to renovate your cabin, you ask the carpenter to give you an offer. The carpenter makes an offer, and is willing to give a 30% discount, since the company is an important customer

Advice: By accepting the discount, you will be exposed to a certain risk. It may be argued that the 30% discount is a bribe offered to you in connection with your job. You should discuss the matter with your supervisor. To be on the safe side, you should not accept these types of services from the company's suppliers.

5.2.3 Trading in influence

Trading in influence is criminalised under many applicable anti-corruption laws. To offer or give an improper advantage to a third party in order to influence the conduct of another is prohibited.

If we engage lobbyists or agents to influence a public body or political decisions, certain precautions must be taken:

- We must try to identify any connections between the lobbyist/agent and politically exposed persons;
- The lobbyist/agent must be open about its engagement for our company in his contact with the decision-makers;
- The fee must be reasonable and proportionate to the service provided by the lobbyist/agent.

5.2.4 Palm greasing

Palm greasing is a concept in the borderline between legal relationship building and corruption. It often takes place as part of an existing relationship, for example by the means of gifts, dinners, entertainment or travel. We must be particularly aware of our role during decision-making processes.

5.2.5 Facilitation payments

Facilitation payments are payments made to expedite decisions and approvals to which the company is legally entitled. This is typically paid to a public servant to secure or expedite routine, non-discretionary governmental actions to which a company is entitled. Such payments are only intended to influence the timing of a decision and not the outcome.

Under some countries' law, facilitation payments are legitimate, while other countries do not distinguish between corruption and facilitation payments. Facilitation payments are still a major challenge in many parts of the world. Getting rid of such payments is a long-term goal that requires the cooperation of governments and other international agencies. Our company has decided to prohibit payment of facilitation payments. Our policy is based on the OECD recommendation that such payments have a subversive effect. If you are ever asked to pay a facilitation payment, you must immediately report this to your line manager.

Typical examples of facilitation payments:

- To pay a small amount to a public servant to obtain permits necessary to conduct business in the relevant country;
- To pay a small amount or give a small gift (as a substitute for money) to port authority representatives to be prioritized in the port;

- To pay cash to customs officers to release goods held in customs;
- To pay a small amount as an unofficial fee to obtain a visa or a work permit, or to pass through immigration or customs at the airport.

We do not prohibit payments made under duress or extortion. If you ever find there is an immediate threat to your health or safety, you should pay and report the case to your line manager afterwards.

Example 2 – Facilitation payments

An oil service company has to import a spare part into an African country, and the part is detained by customs. The spare part is required for the oilrig, and without the spare part, the oil service company may be held liable for a financial loss of several hundreds of thousands of dollars for the oil produces. The customs officer in the African country explains that there is something wrong with the submitted documentation, and that the process may take another two weeks unless he is compensated for the extra overtime work. The oil service company agrees to pay an overtime compensation of USD 2,000, which is paid in cash to the local customs officer.

Legal implications: The oil service company and the involved individuals may be penalised for paying a bribe to the customs officer. The overtime compensation is just another word for a "bribe": a non-transparent, unofficial payment to the local officer personally. A fee for expedited processing paid to the customs officer with an official receipt would have been OK.

5.2.6 Who is considered a public servant?

In most anti-corruption laws, the term "public servant" includes:

- National, regional or local authority employees;
- Officials holding a legislative, administrative or judicial position;
- Officials or agents of a public international organization (e.g. the United Nations, the European Union, the World Bank);
- Political parties, persons employed by political parties and candidates for public offices;
- Any other person who acts in an official capacity on behalf of a government body or agency.

Under certain anti-corruption laws (such as the FCPA), employees in government-owned or government-controlled companies are also considered "public servants". Subsequently, employees in government-owned oil and gas companies are considered public servants under certain anti-corruption laws, and for that reason, it must be carefully considered whether it is appropriate to give gifts or offer hospitality to employees of such companies.

5.2.7 Further guidance on certain activities

5.2.7.1 Gifts and hospitality

Hospitality aimed at improving the impression of the company, presenting our products and services or establishing good business relationships, are important parts of conducting business. Reasonable and proportionate business hospitality expenses may be reimbursed under applicable anti-corruption laws and do not constitute violations of this policy.

However, gifts and hospitality may be abused for corruption purposes. The expenses must meet the general requirements described below and be according to our Gifts and hospitality procedure. This applies both when receiving and offering gifts or invitations.

Hospitality includes meals, travel, accommodation and entertainment. Gifts and hospitality must always be given or offered in a transparent manner and must never be used for the purpose of influencing a decision or negotiation.

Care must be exercised in respect of hospitality involving public servants. Public servants will often be subject to strict rules, and no representative of our company should ever try to influence the decisions of a public servant by using improper methods.

Dilemma 2 – Hospitality
A supplier invites you to attend their annual seminar in Nice. The programme includes one day of presentations and discussions and one day of sightseeing and various outdoor activities. You would like to attend, but not if it exposes you to personal risk.
Advice: You should discuss the invitation with our supervisor. If the company may benefit from your attendance at this seminar, your invitation will probably be approved. However, travel and accommodation expenses will be paid by our company. If the professional content at the seminar is weak, your supervisor will most probably not approve the invitation.

These general requirements apply to all gifts and hospitality expenses:

- All expenses must be in accordance with applicable laws and internal guidelines;
- Hospitality should always take place in a relevant business context;
- Gifts and events should never be extravagant, and must be in accordance with ordinary business practices;
- Gifts or hospitality expenses shall not be given or received during a tendering process;

- Offer of or participation in events that are immoral or unlawful, or that may endanger the reputation of the company shall not occur;
- Cash or cash equivalents should never be offered, given or received;
- When considering whether an invitation to a recipient is improper, both the monetary value and the frequency must be considered.

The Gifts and hospitality procedure contain further guidance on such expenses. Please note the following restrictions that currently apply to self-approval of gifts and hospitality:

- Private sector gifts; not accepted unless preapproved by line manager;
- A working lunch must not exceed NOK 500 per person;
- A working dinner must not exceed NOK 1 500 per person.

5.2.7.2 Engagement of business partners

Purchasing services and business partnerships expose our company to a liability risk on the basis of other parties' violations. Under applicable anti-corruption laws we are expected to seek to avoid unlawful payments from a person affiliated with our company. A person who provides services for or on behalf of our business has such affiliation. Examples are suppliers, subcontractors, sellers, consultants, agents, lobbyists, brokers, financial advisors and lawyers.

Business partners should only be engaged for legitimate business purposes and based on normal commercial terms and conditions. The remuneration should be in proportion to the service performed and be commercially acceptable.

Typical circumstances that may increase the risk of corruption include payment of even amounts, success fees, prepayments and reimbursements of unspecified expenses incurred by the business partner.

We choose our business partners carefully. This involves mapping relevant information relating to the legality of their activities, reputation, experience, technical knowledge, history and potential risks or liabilities.

For some of our business partner, a background check must be performed (integrity due diligence, IDD). In such cases, the criteria for and the scope of the IDD must be included in our procedure. The level and complexity of the review must be in proportion to the risk that exists. Risk factors will typically include:

- The likelihood that the business partner will interact with a public servant on our behalf;
- Whether the services are to be delivered in a country that is perceived to have a high corruption risk;
- Whether the business partner is new to the industry, without any documented history;

- Whether a public servant has tried to influence the company to use a specific local company;
- Whether the company is a private limited liability company, and it is difficult to identify the owners or the ultimate beneficiary owners.

All contracts with business partners must be in writing. We will do our best to include anti-corruption clauses in our contracts to ensure that our business partners are committed to following our standards. If any of our business partners are suspected of anti-corruption law violations in connection with work performed under our contract, the contract must be terminated immediately and further payments suspended.

Dilemma 3 – The local partner

To fulfil the requirement of "local content" in a specific country, our drilling rig company establishes a joint venture with a recently established oil service company. When we contact the Ministry of Petroleum, the Ministry's representative talks very favorably about the new local oil service company. A couple of meetings are arranged with the local company, and they make a good impression even though they need to develop their technical expertise and a more professional organization. They will clearly benefit from the joint venture, both financially and in terms of technical expertise. Can we cooperate with this company?

Advice: A thorough due diligence review of the local company must be performed. That the local company appears to have been preferred by a public servant is a "red flag". The due diligence must disclose who the owners and beneficiary owners of the local company are. If you choose to cooperate with the local company, you have to monitor their work very closely and ensure that expenses appear in the joint venture accounts.

5.2.7.3 Work with agents

Agents or intermediaries function as a liaison between our company and a third party. In international operations or business development, the use of agents, consultants, sales representatives, customs brokers, contractors or distributors, is often unavoidable.

Agents may be used to transfer bribes on behalf of the principal to a third party, and therefore constitute a corruption risk. To work with agents in countries with a high corruption risk, requires due care and attention. If any of our agents pay a bribe, this may result in liability for our business for anti-corruption law violations.

The engagement of an agent to conduct business development must always be approved by the board of directors.

When you engage an agent, you must ensure:

- That a written agreement is concluded;
- That the fee is in proportion to the services provided;
- That the services are entered in the accounts in accordance with generally accepted accounting principles;
- That anti-corruption clauses are included in the contract;
- That you monitor the agent's work.

Example 3 – The agent

A country in Africa has recently discovered new oil reserves, and a European exploration and production company has decided to participate in a tender for oil licences in the country. The country as a reputation for corruption, and it is a common perception that the president of the country may be personally involved in the licensing process. You company has been contacted by an agent in the Middle East that claims to have personal contact with the son of the president of the African country and offers his assistance. To assist, he demands a prepayment of USD1 million, and a success fee of USD 2 million if your company is granted the license. Your company engages the agent and is granted the license, and transfers the fee to the agent's Cayman Islands bank account.

Legal implications: The exploration and production company has most probably paid a bribe to the president of the African country through the agent. Since this is a well-known corruption scheme, the police authorities will not believe you when your explanation that you thought these expenses were suitable fees for lobbying services. They will ask which services were performed that could justify a fee of USD 3 million. In some jurisdictions, the expenses may also be a violation of the prohibition on trading in influence (if no transfer of money from the agent to the president can be proved).

5.2.7.4 Joint ventures

A joint venture will partly be financed by our company and may act on our behalf. Since a joint venture consists of several companies, there is a risk that bribes take place between some of the parties without our knowledge. For this reason, it is important to:

- Perform a risk-based due diligence of all the potential joint venture partners;
- Implement measures in the joint venture to ensure compliance with applicable anti-corruption law;
- Ensure that we are entitled to audit the accounts of a joint venture and that we establish an audit committee with at least one representative from our company;
- Include clauses in the joint venture agreements that entitle us to terminate the partnership in the event of breach by the other partners.

5.2.7.5 Acquisitions

When acquiring shares or assets in another company, we must consider the corruption risk associated with what we acquire. The risk of corruption must be assessed during the due diligence review prior to the acquisition. If a risk associated with the country or the industry is detected, we may choose to perform a due diligence review after the transaction has been completed.

5.2.7.6 Social projects, donations and grants

Making social investments and keeping in touch with local communities are an important part of the company's social responsibility. Unfortunately, there is also a certain risk associated with such expenses. If a social project or a donation disproportionately favors a decision-maker, in either the public or the private sector, the payment may potentially represent a violation of anti-corruption laws. We must always ensure that social projects, donations and grants are awarded according to objective criteria and in order to improve our overall image and reputation. To avoid risk of violation of the law, we expect you to:

- Prepare objective criteria if your line unit plans to participate in social projects or give donations or grants, and act in accordance with these criteria;
- Ensure that a social project, donation or grant does not disproportionately favor a public servant who is important to our operations;
- Ensure that we cooperate with individuals and organizations that are able to use the funds in line with the company's intentions;
- Ensure that we have enough documentation on the investment and that we describe the investment accurately and reasonably detailed in our accounts and records.

5.2.8 Internal procedures

5.2.8.1 Risk assessments

If deemed necessary by the CEO, the CFO responsible for conducting an annual assessment of the corruption risk associated with our activities. As a minimum, the risk assessment must include risk associated with countries, business partners and transactions.

5.2.8.2 Implementation and training

All employees must be given anti-corruption training. Human resources manager is responsible for supervising the training activities in the organization. The frequency and the amount of training will be based on the results of the risk assessment. Certain business units and functions may require more extensive training than what is required for employees in general.

5.2.8.3 Monitoring and review

The CFO is responsible for monitoring the implementation of the Anti-corruption Policy and supplementary procedures. Compliance with policies and procedures must be subject to internal control and supervision. A review of certain activities and expenses must be made to identify potential non-conformances.

5.2.8.4 Handling of reports on violations

We encourage you as our employee to let us know if you ever come across violations of our anti-corruption policy. See our Whistleblower Policy or submit a report to your line manager or the CEO.

A report of possible corruption involving the company must always be made known to the CEO.

The CEO and the board of directors may initiate internal or external investigations to clarify relevant facts in connection with reports of potential corruption. They may also decide to notify relevant public authorities of the findings. Violations of anti-corruption laws will trigger disciplinary action and will result in dismissal or termination.

5.2.8.5 Accurate keeping of accounts and records

All transactions you are involved in must be recorded accurately and reasonably detailed in our accounts and records. If this is not done, it may constitute an independent violation of the law pursuant to applicable statutory provisions.

5.3 Appendix 3; Whistleblower policy

5.3.1 Introduction

The company conducts its business in a professional and correct manner in compliance with the highest ethical standards, internally as well as externally. A good voice climate is a prerequisite for the company's development and promotes a good working environment. We therefore encourage open and honest discussions in the company and will protect our employees' freedom of speech. The management acknowledges that whistleblowing is positive to the company. Knowledge is necessary for correction of and learning from deviations. We want our employees to report any violation of the law, the company's policies and procedures, ethical norms and other censurable conditions.

This will ensure compliance, reduce unwanted behavior and may prevent detrimental episodes. Employees who report unacceptable conditions in the company are therefore a valuable resource for the company.

This policy describes the procedures for reporting censurable conditions and applies to all employees and hired contractors. You have a right to report censurable conditions in the undertaking. However, the whistleblower must proceed responsibly when making such notification and must therefore comply with this policy.

An employee who reports censurable conditions must never be subjected to any form of retaliation, neither disciplinary nor any other negative reactions from the company as a result of the whistleblowing.

5.3.2 Notification procedure

5.3.2.1 When should you report an issue?

You are encouraged to report censurable conditions in the undertaking. Censurable conditions are conditions that are contrary to rules of law, our code of conduct, internal procedures and policies or ethical norms that are widely accepted in society. The conditions may affect employees, suppliers, customers, the company itself or the general public. However, the policy has not been prepared for employees to raise questions regarding the company's financial or business decisions.

You have a general duty to notify if you suspect a criminal offence or practice that may put anyone's life or health at risk. You must always report incidents of non-compliance with the company's values as they are expressed in our code of conduct, and of issues that may significantly harm the company's reputation.

Examples of censurable conditions you should report are:

- Danger to life and health, including violation of security and protection procedures;

- Unsafe working conditions, including violation of applicable employment law related to the working environment and safe working conditions;
- Harassment, discrimination, unfair employment practice or abuse of alcohol, narcotics or other intoxicating substances;
- Violation of competition legislation;
- Threats to the climate and environment, including violation of environmental legislation;
- Corruption, fraud or other economic irregularities.
- Violation of privacy.

5.3.2.2 You must proceed responsibly when making a notification

You should proceed responsibly when reporting a censurable condition. Which procedure you should follow depends on the circumstances and the nature of the censurable condition. The notification can be made orally as well as in writing.

An internal notification in accordance with this policy will always be responsible. We encourage all employees to always notify internally. Internal notification can be made to your line manager, an employee representative or others in the company, or to an external recipient if offered by the company.

Who should you notify in the company?

- You should always first notify your line manager, who can take the case further on your behalf.
- If it is likely that your line manager is involved in the censurable condition, you can notify any other person who is qualified to investigate the matter. You can, for example, notify the company's CFO of economic irregularities or the company's HR director or an employee representative of concerns regarding employment matters.
- You can also report to the Human Resources manager (the company's appointed whistleblower investigation officer/compliance officer). The Human Resources manager will also be able to answer general questions regarding the company's whistleblower policy.
- An employee may also notify the chair of the company's board directly if the employee believes that notification to his/her line manager or Human Resources manager will not result in an adequate investigation of the employee's concerns.

How to notify

You should make it clear that you are reporting an issue in accordance with the company's whistleblower policy, for example by marking all written correspondence "confidential". This will ensure that the recipient understands that this is a notification according to this policy, and that the recipient must take the necessary steps to investigate the matter and protect your identity. The person who receives a

notification must register the date of the notification and prepare a report describing the censurable condition concerned.

Notification in accordance with this policy will be treated confidentially. Only persons taking part in the follow-up will be informed of the subject matter of the notification. However, in the further investigation of the matter it may become clear to other employees who the whistleblower is. You can also be asked to make a statement. If it is likely that your identity will be revealed, you will be informed as soon as possible.

We understand that you can find it hard to report particularly sensitive problems or matters that concern your colleagues. If you choose to notify anonymously, it will generally be more difficult to investigate the matter efficiently.

If the notification concerns other employees, they are also entitled to protection and to be informed of the matter. The company will handle, store and delete all personal data that are received, collected or registered under this policy in accordance with applicable personal data legislation.

5.3.2.3 How should the company react when notified

As an employer, the company shall ensure that the notification is adequately investigated within reasonable time. The company must ensure that you as a whistleblower has a thoroughly sound working environment. If necessary, the company must adopt necessary measures to prevent retaliation.

All notifications made in good faith will be investigated. The investigation will normally be made by a small investigation team from the company. If the notification concerns serious accusations, the company may decide to engage external resources to assist in the investigation. You will receive a written response to our notification as soon as possible. The company will implement preventive measures if its assessment of the notification indicates that such measures are required. If the company concludes that there is no reason for concern, you will receive an explanation of the company's conclusion.

A notification may have consequences for those involved in violations, and the company can choose to report the matter to relevant public authorities.

5.3.2.4 Prohibition against retaliation

All forms of retaliation against a person who has notified in a reasonable manner are prohibited under this policy and applicable local legislation.

Illegal retaliation includes formal and informal sanctions and improper conduct towards you as an employee or hired contractor.

You will never experience use of disciplinary decisions or other negative reactions, such as a warning, dismissal, summarily dismissal, suspension, change of duties or relocation as a result of the notification. Nor should you experience threats,

harassment, exclusion, unfair discrimination and similar improper conduct. This applies even if you were wrong, if you notified in good faith.

[Whistleblowers in the UK are protected by the Public Interest Disclosure Act 1998, PIDA against being punished for public disclosure of certain serious concerns that are of interest to the general public. Information pursuant to the PIDA should be sent to the public bodies as prescribed by the Act.]

Companies operating outside Norway should seek local legal advice about this policy in order to ensure compliance with local whistleblower requirements.

5.4 Appendix 4; Gifts and Business Hospitality Procedure

5.4.1 Introduction

This procedure applies to the following situations:

- When you are planning to give a gift on behalf of the company to a person in the private or the public sector;
- When you receive a gift in connection with work;
- When you are invited for a meal, a business trip or a company event in connection with work; or
- When you are planning to invite a person in the private or the public sector for a meal, a business trip or a company event in connection with work.

Since such expenses may be abused for corruption purposes, it is important that you understand and comply with this procedure. Reasonable and proportionate hospitality expenses are not prohibited under applicable anti-corruption law.

The Human Resources manager is responsible for implementing and monitoring the gifts and hospitality procedure.

The procedure consists of the following elements: (i) a general checklist and (ii) limits for self-approval and further guidance. Expenses for gifts and hospitality that exceed the limits for self-approval, must be reviewed the CEO in each case.

5.4.2 General checklist

These general principles apply to all company gifts and hospitality:

- All expenses must be in accordance with applicable law and internal guidelines;
- Hospitality should always take place in a relevant business context;
- Gifts and events should not be extravagant, and should be in accordance with general business practices;
- Gifts or hospitality expenses should not be given or received during a tendering process;
- You must never give or accept invitations that are immoral or illegal, or that may entail a risk of damage to the company's reputation;
- Cash or cash equivalents should never be offered, given or received;
- When assessing whether an invitation to a specific recipient is improper, monetary value and frequency should be taken into consideration.
- You should pay travel and accommodation expenses for your spouse, family members or friends if you decide to invite them to business events or trips.

5.4.3 Limits for self-approval and further guidance

5.4.3.1 Gifts

If a gift or hospitality expense is unacceptable pursuant to the general checklist, you may give and receive gifts and other hospitality in accordance with the limits indicated below.

The private sector:

- You cannot receive or give any gifts. If deemed impolite not to accept a gift the CEO should be notified;
- You may receive gifts of obvious low value; such as flowers, a book or small promotional items (e.g. with the company's logo), without requesting the value of the gift.

If it is likely that refusing a gift would be perceived as an insult or it would harm business relations between the companies, you may accept the gift and give it to the CEO as soon as possible.

The public sector:

- You should not give gifts to public servants.
- Nevertheless, you may give gifts to public servants if:
  - you are in a country in which modest gifts are a part of a recognized and well-established tradition, and it is considered manifestly rude not to bring a modest gift;
  - ceremonial gifts in connection with public holidays are expected according to local tradition (e.g. Ramadan, Eid). It is assumed that the value is less than NOK 200 (*This limit may be adjusted, and we request you to set a limit that reflects the typical value of such gifts in the country in which you operate*). You should always seek local law advice before giving someone such a gift;
  - according to local traditions, one is expected to bring a gift to the head of a delegation from a private sector company or a public body. It is assumed that the value of the gift does not exceed NOK 400 (or local currency equivalent) and that the exchange takes place during a public meeting or a company event.

5.4.3.2 Meals

The private sector:

- You may host a working lunch at a cost of up to NOK 500 (or local currency equivalent) per person, or a working dinner with a cost of up to NOK 1,500 (or local currency equivalent) per person.

The public sector:

- If there is a legitimate need for inviting a public servant to a meal (for example in connection with a visit to our offices, inspections or a conference sponsored by us), you may host a working lunch at a cost of up to NOK 500 (or local currency equivalent) per person, or a working dinner at a cost of up to NOK 1.500 (or local currency equivalent) per person. The criteria of business context must be strictly applied to public servants.

5.4.3.3 Travel

Payment of reasonable and documented travel expenses for public servants in accordance with national law or orders from authorities may always be paid by the company. If it is necessary to arrange transportation in connection with an inspection, a meeting or another business-related event in the country in which you operate, you may arrange for transportation for one person from the private or the public sector.

You cannot arrange transportation yourself or cover expenses for overnight stays for business partners or public servants when travelling abroad without the approval of the CEO. This does not apply if we have a contractual obligation to refund travel and accommodation costs for some of our business partners.

If you are invited to an event abroad, and the CEO approves the invitation, our company will cover your travel and accommodation expenses during the event.

You are not allowed to pay the per diem allowances of anyone outside our company without the approval of the CEO.

5.4.3.4 Entertainment

You may not invite - or accept an invitation - to an entertainment event without the approval of the CEO. Some of these events may be useful networking opportunities for our employees. If the event is too extravagant, has limited professional content, appears to be inappropriate or liable to create an improper influence, you will probably not obtain approval to attend the event.

5.4.4 Control measures

The Human Resources manager shall keep a register of gifts and hospitality expenses. All offers and all acceptance of gifts and invitations to or from the company shall be recorded.

Expenses for gifts and representation shall be recorded accurately and correctly in the register.

5.5 Appendix 5; Integrity Due Diligence Procedure

5.5.1 Introduction

The purpose of this procedure is to describe Eureka Group's objective and efforts to reduce risk in relation to business partners. The process of reviewing and assessing the risk related to business partners is referred to as a background check, an integrity due diligence or IDD. The term "business partners" includes all enterprises or individuals our company enters into a business relationship with, including suppliers, consultants, agents, joint venture partners and other intermediaries.

A key principle of our Code of Conduct is to choose our business partners carefully. Our background checks shall be risk-based, which means that we cannot use the same process on all business partners. The thoroughness of the review will be decided based on a step-by-step approach, which is described in this procedure.

The CFO is responsible for implementing and monitoring the background check procedure.

This procedure refers to the organization Transparency International's ranking of the countries' level of corruption (the Corruption Perceptions Index). The most recent version is available at www.transparency.org.

5.5.2 Integrity due diligence

5.5.2.1 Initial red flag assessment

If you are responsible for choosing a new business partner, you first have to conduct an initial assessment of the potential partner's reputation, capability and experience. That means to search for and review all relevant information about the company, the management and the board of directors, as well as relevant areas associated with the company, such as financial information, media profile, company history and corruption risk in the country in which the company is incorporated and operates. In this work, you should look for potential "red flags" related to a new business partner. Examples of "red flags" are:

- ⇨ The business partner is a new enterprise, and it is difficult to identify the owners of the company or the individuals who has the ultimate control;
- ⇨ The business partner has a very complex corporate structure and has a parent company or operating units in countries that are known for secrecy laws or are considered "tax havens" (examples are Panama, the British Virgin Islands, the Cayman Islands);
- ⇨ The company and/or its management have recently been investigated for violations of anti-corruption laws;

- ⇨ The company and/or its management have recently been involved in scandals related to "social dumping" or human rights violations;
- ⇨ The company is registered in a country subject to trade restrictions and/or anti-terrorist laws;
- ⇨ The business partner is presumed to have family ties or business ties with government officials or politically exposed persons ("PEP");
- ⇨ A public official has exerted pressure to persuade someone in our company to use a specific business partner;
- ⇨ The business partner states that it has influence through relations with politically exposed persons in a country considered as being exposed to significant corruption risk, and asks for large prepayments, a lump sum or success fees that are not reasonable in terms of the services to be provided;
- ⇨ The business partner requests payments to be made to another company and/or to bank accounts in a country that has no connection to the business partner or the provided services;
- ⇨ The business partner is unwilling to cooperate during the background check process and does not accept standard declarations and contractual provisions on business conduct.

The list of red flags is not exhaustive, and you must exercise your best discretion to identify risks based on open sources such as the internet, media and information from our business affiliates. The identification of a red flag does not necessarily mean that we cannot engage the company, but it means that an additional review is required to reduce the risk. We should never choose a business partner that does not abide by acceptable standards for ethical business conduct.

5.5.2.2 Situations in which a background check is not required

If no red flags have been identified and the business partner or the transactions fall under any of the categories below, a background check is not required. We have decided to exclude the following from the background check procedure:

- ⇨ Transactions with companies listed on a stock exchange in an EU state, an EEA country, Canada or the USA;
- ⇨ Transactions with suppliers that sell goods (equipment, hardware, machines, etc.) on the basis of standard price lists;
- ⇨ Contracts with a value of less than [USD 300.000] a year in a country that scores more than 50 points on Transparency International's corruption index;
- ⇨ Contracts with a value of less than [USD 20.000] a year in any country, with the exception of contracts with agents or intermediaries that perform work in connection with public authorities. For agents involved in business development and/or work with authorities, a background check must always be performed.

[Instructions – the scope of the list is just a suggestion and should be adjusted on the basis of the company's profile. The purpose of the list is to make exceptions for low-risk contracts and transactions.]

5.5.2.3 Implementation of background checks

The purpose of a background check is to collect key information about a business partner and analyze and assess any "red flags" that come to light.

Alternative 1 (for companies that do not have the capacity to implement a background check):

If a background check is required under this procedure, the CFO must order a report from a supplier that performs background checks of companies.

(These reports may be ordered from Kroll, Frank Partners, audit and consultancy companies such as KPMG, PwC, Deloitte, etc.)

You also have to ask the business partner to fill in our standard due diligence form. The completed form must be filed together with the signed version of the contract.

A background check may take approximately two weeks, and enough time must be set aside to obtain important information about the business partner.

Alternative 2 (for companies that perform part of the background check using own resources)

A background check will include the following actions:

0. The business partner must fill in our standard due diligence form, which provides us with information about the owners, company history, current policies, code of conduct, etc.;
1. Searches for information about the business partner, its management and board members in databases such as World Check, Dow Jones Risk & Compliance and similar, or in open sources (Google, press coverage, business registers on the Internet, etc.);
2. If red flags still are present, or if key information about the business partner cannot be confirmed, an extended report from an external supplier should be ordered.

When implementing a background check, it is important to make continuous assessments of whether the obtained information is reliable and relevant to the risk related to the business partner. How much time that should be spent on the review, should be decided based on contract value, our own company's exposure and the information that comes to light in each case.

5.5.2.4 The result of the background check

The CFO and the line manager for the responsible business unit should review the result of a background check and decide whether the business partner should be categorized as "approved" or "not approved". If a background check has not removed all the "red flags", the decision to engage the business partner must be made. In some cases, external legal advice may be required. In certain cases, we may engage a

business partner although certain "red flags" have been identified in a background check, but with further measures to mitigate risk and with increased follow-up of the contract.

The business unit finance manager is responsible for keeping a record of the results of background checks, which is available to all employees involved in engaging a new business partner.

A background check is valid for two years, but the Eureka Group CEO may decide that it should apply for a shorter or a longer period.

5.5.3 Measures to mitigate risk

For certain business partners, measures to mitigate risk and extra follow-up should be actively used to ensure compliance with laws and ethical business conduct. Such risk-mitigating measures includes, to:

- ⇨ Request all business partners that provide services (agents, consultants, etc.) to comply with our Code of Conduct;
- ⇨ Use contractual clauses related to anti-corruption, trade restrictions, work standards, etc. and monitor the compliance of such contractual clauses;
- ⇨ Require compliance/anti-corruption training for certain business partners;
- ⇨ Require the privilege to audit the business partner;
- ⇨ Ensure that we are entitled to rescind and entitled to suspend further payments if irregularities are suspected;
- ⇨ Perform a thorough review of invoices and the work performed by the business partner.

5.5.4 Privacy in connection with background checks

Although information collected during a background check usually are associated with a company and not individuals, a background check will generally include the processing of personal data.

We must ensure that all personal data collected under the IDD procedure is adequate, relevant and not excessive in relation to the purpose for which it is collected. The categories of personal data to be collected and processed in connection with this review will vary depending on the individual case. The company may in this context process sensitive data, including information on suspected criminal behavior, e.g. violations of laws pertaining to accounting, bribery, corruption, discrimination and health, the environment and safety. Furthermore, we may process information on whether employees or consultants have any connections to government agencies or political parties. Although such data cannot be considered sensitive under applicable data protection law, we must aim at treating it as sensitive.

The result of a background check will be shared on a need-to-know basis. Only information on whether a business partner will be approved or not approved will be available to employees with access to the background check records. Associated documents and reports will be retained by the CFO and will only be shared with employees who have a work-related need to access these documents.

[The following paragraph may be used by HitecVision's Norwegian portfolio companies]

*The processing of personal data by the company requires a legal basis described in EU Regulation 2016/679 (the "**GDPR**") articles 6, 9 and 10.*

Processing of personal data in connection with background checks is based on the following:

- *Legal basis, cf. the GDPR article 6 no. 1 letter c, the GDPR article 9 no. 2 letter b, the GDPR article 10: the Penal Code section 387, the Compensatory Damages Act section 1-6, the UK Bribery Act and the US Foreign Corrupt Practices Act.*
- *Necessary for the performance of an agreement to which the data subject is a party, cf. the GDPR article 6 no. 1 letter b and the GDPR article 9 no. 2 letter b: Our company needs to ascertain that our contract partners act in accordance with applicable laws and regulations.*
- *Necessary to safeguard a legitimate interest, cf. the GDPR article 6 no. 1 letter f:*
  Our legitimate interest in fulfilling our legal, social and ethical responsibilities overrides the regard for the data subject's privacy.
- *Necessary to establish, assert or defend a legal claim, cf. the GDPR article 6 no. 1 letter c, the GDPR article 9 no. 2 letter b, the GDPR article 10:*
  We need access to information that is relevant to defend potential allegations of misappropriation.
- *Permission from the Norwegian Data Protection Authority:*
  We will apply for and maintain a permit from the Norwegian Data Protection Authority to the extent necessary for our processing of personal data. If granted, the permit may constitute an additional legal basis.

Personal data that we collect for the purposes of a background check, cannot be stored any longer than is necessary for the purpose of the processing, cf. the GDPR article 5 letters b and e. To the extent possible, the personal data shall be stored separately from other information to be able to meet the retention period requirement.

When personal data on business partners no longer is required, it must be deleted. The assessment of how long this must be made in each individual case. Personal data related to the background check may be stored for a maximum of three years, with reference to the ordinary limitation period, unless the information is required in connection with ongoing legal proceedings or investigations, or unless further retention is required to comply with the law. Retention of personal data for more than three years must be approved by the CEO.

Personal data related to background checks in connection with agent agreements or similar may be stored as long as the agreement is effective and may be stored for a maximum of three years after the expiry of the agreement with reference to the ordinary limitation period.

Before a file containing a background check is deleted, it must be reviewed to ensure that the contents complies with the guidelines. The indicated retention period has been set with a view to ensuring that this information is available within the penal code provisions on limitation periods in Norway, the United Kingdom and the USA.

Due diligence form

[COMPANY NAME] DUE DILIGENCE OF BUSINESS PARTNERS

Please fill in the questionnaire below and enter NA if the question is not applicable to the company.

1. **The company's name:**

2. **Contact details:**

Address:	**Telephone:**
	Telefax:
	E-mail:
	Website:

3. **Information from the register of business enterprises (if relevant)**

Business registration number:

Date of registration:

Expiry date:

Register:

Place, country:

Organization number and country:

Please enclose copies of any registration documents or other documentation required under local law for the company to be granted permission to conduct business. Also, enclose a copy of the documentation that shows the company's establishment or incorporation.

4. **Number of company employees: _____**

5. **Is the company or the parent company listed on the stock exchange in the USA or Europe? Yes_____ No _____ . If Yes, please state the name of the stock exchange and provide listing information:**
   _____

6. **Enter bank or financial references:**
   _____
   _____

7. **Describe the legal structure of the company (e.g. limited liability company, partnership, privately owned company, other) and enter the name of any parent company, subsidiary or associated company:**
   _____
   _____

8. **Enter all the members of the board of directors of the company:**
   _____
   _____

9. **Indicate all other persons who may exercise control over the company through any type of arrangement:**
   _____
   _____

10. **Please describe the company's active management, with names, addresses and nationality, as well as any ownership interests in the company:**

Name and address	Nationality	% ownership interest

11. **Indicate all owners with names, nationality and percentage ownership interest. Please also provide the identity of the ultimate beneficial owners:** (*Note*: If an owner is a company, please state the name, nationality and ownership interest of the owners so that all ultimate owners or beneficial owners are identified. The sum of the ownership shares must be 100%. If the company is listed, please identify all shareholders who own more than 5%.)

Owner names (legal and beneficial owners)	Nationality	% ownership interest

12. **Please indicate the names of key personnel or executive employees:**

Name	Nationality	Position/Role

13. **Please provide the company's accounts or appropriate alternative financial information for the past two years (audited, if available), including the balance sheet and the income statement. If the accounts are not available, please explain why and provide alternative financial information that is reasonable and relevant.**

14. **Please submit a copy of the company's Code of Conduct, Ethics Policy or similar.**

15. **Please provide the name and contact details of the Chief Compliance Officer of the company, or a manager with a similar role.**

16. **Does any public servant have ownership, financial or other direct or indirect interests in the company?**

    If yes, please indicate the name of the public servant(s):

17. **Is or was a close relative or business associate of a public servant owner, board member, trustee or employee of the company, or has any owner, board member, trustee or employee of the company a close relative who is a public servant?**

    If yes, please indicate the person's position, the name of the person who held the position and the person's association with the owner, board member, trustee or employee of the company:

18. **Over the past five (5) years, the company (including an affiliate or former affiliate or predecessor), a board member or an executive employee of the company has been: (1) suspended from business for any reason, (2) investigated, prosecuted or convicted for any violation of laws or regulations, or (3) subject to allegations of fraud, misrepresentation, money laundering, bribery, corruption, tax evasion or other related fraudulent or corrupt practices?**

    If yes, please provide details:

I have reviewed this questionnaire and am authorised to reply to the questions and provide the information requested. I declare and confirm that the information provided is correct and complete and that it has been provided to the best of my ability.

_____

Name:

Date:

Position:

Company:

5.6 Appendix 6; Sanctions Compliance Policy

5.6.1 Introduction

Our policy entails strict observance of all applicable laws relating to trade restrictions and the fight against terrorism. The policy is not exhaustive, but provides an insight into and an overview of the legal framework in this area. The trade restrictions relate to cross-border trade in products, money, technology and services. In order to avoid violations of sanctions for the company, it is important to comply with the high standard set by the company through this policy.

You have to familiarize yourself with applicable sanctions rules and follow the procedures described in this policy. The purpose is to minimize the risk of violations of applicable economic sanctions and trade restrictions in connection with our operations.

In this policy, "business activities" include investing, financing, concluding contracts, operating, performing services, exporting and importing, as well as other similar activities.

Our business partners may expose us to risk by violating trade restrictions and applicable legislation, for example anti-corruption legislation. Therefore, this policy must be read in conjunction with our *IDD procedure,* which describes the procedure for investigating business partners and taking control measures. Business partners include our contractors, customers, suppliers, consultants, agents, joint venture partners, lobbyists and other intermediaries and third parties involved in a transaction.

The CFO is responsible for implementing and following up the Sanctions Compliance Policy.

5.6.2 Legal framework

Economic sanctions and trade restrictions are measures implemented as a foreign policy response to situations that create international concern.

Trade restrictions are penalties or restrictions imposed by a country or a group of countries against another country. The restrictions tend to take the form of import duties, prohibitions on exports or imports of certain goods and technologies, arms embargo, prohibitions on investments or restrictions on the transfer of funds and financing, or other administrative regulations.

In addition to the restrictions imposed on countries, there are international trade restriction rules that may restrict transactions with certain individuals, companies, entities, groups, organizations, etc. This may occur, among other things, on suspicion of complicity in promoting terrorism, unlawful arms trade, organized crime, proliferation of weapons of mass destruction, human rights violations, suspicion of opposing democratic processes in certain countries or suspicion of affiliation with certain governments, such as the former governments of Libya and Liberia.

Two examples of such lists are «Specially Designated Nationals», see *http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx* and the EU's consolidated list of individuals, groups and entities subject to EU trade restrictions, see *http://eeas.europa.eu/cfsp/sanctions/index_en.htm.*

Sanctions to fight terrorism includes, for example, an obligation to freeze bank accounts or financial instruments controlled or used by individuals affiliated with al-Qaida, Taliban or other terrorists/terrorist groups.

The sanctions mainly belong to three different categories:

- ⇨ Sanctions that incorporate UN Security Council decisions into national legislation;
- ⇨ Sanctions adopted by the European Union as part of the common foreign and security policy, see *http://eeas.europa.eu/cfsp/sanctions/index_en.htm*, and
- ⇨ US sanctions monitored by the U.S. Office of Foreign Assets Control (OFAC), see *http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx*

In addition, applicable national legislation and trade restrictions must be complied with.

5.6.3 Company policy

Our policy entails strict compliance with sanctions adopted by the UN Security Council, the EU Council and the US authorities. This applies although our company is located outside the EU. Certain company guidelines are a result of requirements from our investors.

Our company shall not:

- ⇨ Engage in business activities that result in violation of applicable trade restrictions or export control regulations.
- ⇨ Engage in business activities with individuals or legal entities listed on sanctions lists introduced by the UN, the EU, Norway or the US.
- ⇨ Engage in business activities with a company that is on the list of companies excluded from the investment universe of the Norwegian State's Sovereign Wealth Fund without the prior consent of Director Compliance of HitecVision, https://www.nbim.no/en/responsibility/exclusion-of-companies/[1].
- ⇨ Engage in business activities with any individuals or legal entities or incorporate entities, in Iran, without the prior approval from the Director of Compliance at HitecVision
- ⇨ Engage in business with companies located in, owned or controlled by the government of a country subject to OFAC sanctions without the prior consent of Director Compliance of HitecVision.

[1] Applicable for portfolio companies of fund VII

- ⇨ Engage in business with a company domiciled in or associated with the Middle East or North Africa without the prior approval from Director Compliance of HitecVision [2];
    - "Middle East" and "North Africa" mean Algeria, Bahrain, Egypt, Iraq, Israel, Jordan Kuwait, Lebanon, Libya, Morocco, Oman, Palestine, Qatar, Saudi Arabia, Sudan, Syria, Tunisia, United Arab Emirates and Yemen.
- ⇨ Invest in a company that conducts business in violation of applicable sanctions regulations.
- ⇨ Invest in a company that produces, proliferates or sells weapons or other military equipment to Myanmar.

Should you ever have any doubts about the sanctions that must be observed by our company, please consult the CFO.

Violations of trade restriction regulations is a criminal offence, and such violations may result in the company or the employees being subject to investigation. Both intentional and unintentional/negligent violations may be punishable pursuant to applicable regulations.

The penalties that may be imposed on the company and its employees are severe and includes fines and imprisonment. A charge may also significantly damage the company's reputation.

Violation of this policy may result in dismissal or have other consequences for your employment.

5.6.4 Responsibility

If you are responsible for a business activity of a global nature, you have to be familiar with this policy, exercise good judgment and do your best to ensure that it is complied with.

In our company, *the CEO* has the following responsibility:

- ⇨ Keep abreast of applicable sanctions regulations, particularly related to Russia, China and Iran;
- ⇨ Conduct regular risk assessments related to contracts, transactions and countries in which we operate to understand the risk of trade restriction violations and export control regulations;
- ⇨ Perform screening against lists of sanctioned individuals and legal entities using World Check or similar databases;
    - The screening should include individuals (as well as other key individuals such as board members and managing directors) and/or the relevant legal entity, including related companies (parent, sibling and subsidiary)
- ⇨ Obtain legal advice from external legal advisors when necessary.

[2] Applicable for portfolio companies of fund VII

Nevertheless, it is everyone's responsibility to ensure that we never conduct business with countries, organizations and individuals listed on applicable sanctions lists or that are excluded according to this policy.

If you think a transaction may involve an individual or a country comprised by sanctions regulations, you must notify the management immediately.

You must never conclude an agreement or carry out a transaction with a company without first ensuring that you know who has final control of the company or who the ultimate beneficial owner of the company is.

If you plan business activities in a country or a region with political and/or military unrest, contact the CEO. An assessment will then be conducted of the potential risk of violating trade restrictions and the relationship with human rights, terrorism and other mapped risk situations.

5.7 Appendix 7; Cyber Security Policy

5.7.1 Introduction

This procedure describes the guidelines all employees must follow to comply with the company's data security objective.

Our overall ambition is to act in a manner that reduces the danger of the company being attacked by hackers. The guidelines' purpose is to set limits in order for the company to be able to maintain data confidentiality, integrity and availability, including identifying attacks, detecting threats and protecting our systems. First and foremost, the procedure contains preventative measures that reduce the risk of attacks, and consequently does not contain information on how the company may recover from a potential attack.

It is important that these guidelines are complied with and used as a guide on a daily basis. The checklist will also apply to board members, owner representatives, independent contractors and consultants, temporary employees and hired personnel. We consequently expect you to read these guidelines and, upon request, confirm in writing that you will comply with them.

Hackers attack in order to change, destroy or steal sensitive information, blackmail users for money or disrupt regular business processes. There are different types of data security threats. These include, among others, the following:

- Malware: Harmful software that is used to harm a computer user. Examples: Data virus, worms, Trojan horses, spyware, adware.
- Ransomware: A type of malware that locks the user’s files, usually though encryption, and that demands payment to decrypt and unlock the data system.
- Social engineering: Probably the most used method of hacking, in which the hacker obtains access by deceiving the user. The hacker often uses charm to obtain sensitive information he otherwise would not have had access to.
- Phishing: A form of fraud which involves false e-mails that looks like e-mails from recognized sources. The intention is to steal sensitive data, for example credit card or log-in information.

5.7.2 Checklist

1. Password Policy

- Use "strong passwords"
  - The password ought to be as long as possible, with a combination of several words or at least 9 characters.
  - The password should include both numbers, symbols, spaces and capital and small letters.
  - The password should preferably not include words or numbers that may be associated with you or the service to which the password applies.
  - Tip: Create the password in sentences rather than individual words.
- Create a unique password for each website or user account.
  - Do not use the same password for all areas as this will provide the hackers with easier access to several areas.
- Use two-factor authentication when possible.
  - Should the hacker get hold of the password, a two-factor authentication will require an additional code, which means that unless the hacker also knows the additional code, he will not gain access to the system.
- Change passwords often and immediately if you suspect that the password may have gone astray.
  - The password should also be changed at first login.
- Never share the password with anyone, whether in writing or orally or with colleagues or family.
- Avoid writing your passwords down, even as a reminder to yourself.
  - Use a Password Manager instead to create and save passwords.
- In the event of accidents or suspicion of a security breach, change your password immediately.

2. E-mail Policy

- Always check the sender address. In many cases, the sender address is different from the actual address.
- If you are uncertain about the sender or the contents, be careful and evaluate the e-mail carefully before clicking on it.

- Be skeptical if the e-mail requests personal or financial information. Therefore, evaluate the sender and the websites carefully before providing information.
  - Be aware that such requests not always will come from strangers – often they come from friends or colleagues. Therefore, contact the sender via other means of communication to ensure that the request is genuine.
  - If the request comes from a reliable company, but you are uncertain about the contents of the e-mail, forward the e-mail to the company's IT department to double-check the validity.

- Be aware of random requests, grammatical errors and clickbait contents. Malware, such as viruses, wants to appear generous by offering the user something, often something that has little to do with work.

- If the e-mail contains links:
  - Never click on a link if you are uncertain about the sender or the contents.
  - By hovering over the link, the URL comes up and it is possible to identify the contents of the link.
  - Please note that clicking these links may cause automatic installation of unwanted codes on your computer, which in turn may cause hackers to access sensitive information.
  - Check if the address is misspelt or whether it ends in ".com" instead of ".no", etc.
  - Do not blindly trust a website that begins with https://. An encrypted and secure connection to a website (https:// and padlock) basically guarantees a secure connection without monitoring. That the page is secured with "https" therefore does not say anything about the site's reliability. Many are unaware of this, and an increasing number of phishing sites use "https" to abuse people's trust.

- If you are going to send a document via e-mail, add the document as a link in the e-mail rather than as an attachment.
- If you receive an e-mail with an invoice from someone claiming to be one of our suppliers, telling you that they have changed their account number, call the supplier and double-check that this is the case.

3. Security updates

- Do not ignore the security updates for Windows and the applications on your computer.
  - Although such reminders may seem like an unwelcome interruption, the software updates implement important security functions to prevent new attacks.
- Check that the fire wall and the anti-virus programme are updated on your computer.

4. Back-up

- Ensure that your files are saved to a server area with back-up procedures, possibly to the company's cloud services
- Avoid unnecessary local saving. If you save files locally on your computer, ensure that you keep a copy of these files on the service area or possibly on the company's cloud services.

5. Working while travelling

- Be careful with what you work on in public, both on PCs, mobile phones and tablets. Use privacy screen protectors if possible.
  - Sensitive information may easily go astray by people sneaking a peak/sneaking a listen.
- Lock the screen on PCs, tablets and mobile devices every time you leave your seat. Also make sure that the device locks automatically when inactive.
- Ensure that all devices (PC and mobile devices) are encrypted. This prevents loss of data if the device is stolen.
- Preferably use mobile data instead of unknown wireless networks.
- USE VPN (encrypted and private network) to connect to the company's network.
- Only bring the data if you need it on the trip.
- Do not leave PCs or mobile phones unattended in public spaces.
- Always check the Ministry of Foreign Affairs' advice before travelling to security risk countries. Information on countries at risk of data attacks are also included here: https://www.regjeringen.no/no/tema/utenrikssaker/reiseinformasjon/id2413163/

6. In the event of attacks

- Turn off the computer immediately and report security breaches and incidents to the closest supervisor or the IT Security Officer.

7. Other procedures

- Only install approved, legal and serious software.
- Avoid sensitive browsing, such as online shopping or logging on to an online bank in the workplace
  - If this is done on behalf of the company, this must be done on the company's devices and on secure networks. Always check with a supervisor first.
- Be careful about using and connecting external devices, such as hard drives, memory sticks and smartphones, to your computer, these may infect the device when connected.
- Be careful about what you share on social media, both privately and on the company's account. Hackers may gain insight into sensitive data that is shared unconsciously.

- PC screens will lock after 4 minutes of inactivity.
- Alle removable devices (e.g., USB, external hard drives etc.) are automatically scanned for malware when connected to a PC.

8. Cyber Security in Automation Solution Projects

Eureka Pumps AS is compliant with the internationally recognized standard NEK IEC 62443 2-4: Security for industrial automation and control systems. There are specific policies, procedures, and documentation to follow for projects that must follow the standard. The involved areas mainly relate to the Electro department, who will receive additional cyber security training, along with the HR and Procurement department.

A Cyber Security Expert will be appointed to each project to ensure compliance to the standards requirements.

5.8 Appendix 8; Data Protection Policy

5.8.1 Objective

We are committed to protecting the privacy rights of our employees and everyone with whom we do business. The objective of this document is to provide a Policy on how to handle personal data in accordance with applicable data protection law. This includes the EU General Data Protection Regulation 2016/679 (the **"GDPR**").

The Human Resource manager is responsible for the implementation and monitoring of the procedure.

5.8.2 Regulatory requirements

5.8.2.1 Territorial scope

For the purpose of establishing a uniform approach to data processing in the company this Policy will generally be observed throughout the company and our group, irrespective of whether or not the GDPR applies.

We may consider local guidelines to this Policy in the following instances:

- If local law in EEA countries in which we operate supplements the GDPR, such as in the field of employment, or with respect to data relating to criminal convictions or offences.
- If local law in non-EEA countries in which we operate imposes additional, stricter or less strict privacy rules, compared to the GDPR.

5.8.2.2 Material scope

This Guideline applies to the processing of personal data wholly or partly by automated means. It further applies to non-automated processing of personal data that forms part of a filing system.

Personal data is any information relating to an identified or identifiable natural person (‘data subject’). "Any information" means just that, *any* information, whether objective facts or subjective opinions. "Relating to" means that one of these elements are present:

1. Content. The information is *about* the person.
2. Purpose. The information is, or is likely to be, used to evaluate, treat in a certain way, or influence the person.
3. Result. The use of the information is likely to have an impact on a person's rights or interests.

"Identified" or "identifiable" means that a person may be identified, directly or indirectly, by reference to an identifier such as a name, ID number, location data, online identifier, or one or more factors specific to a person.

In such assessment, account should be taken of the means reasonably likely to be used to identify someone from the data. A mere technical possibility of singling out individuals from one or more data sets does not in itself make the information personal data, if the exercise is costly or time consuming, or if we are unlikely to perform such exercise.

Example: Employee number, or combination of age, gender, nationality and position.		
Processing	Any operation or set of operations, which is performed on personal data.	Basically, it means any use of data. *Examples: Collection, recording, storage, alteration, transmission, and erasure.*
Automated	That the processing of personal data is performed wholly or partly electronically.	This covers data stored on any electronic medium. *Examples: Files, e-mails, sound recordings, video recordings (provided that they contain personal data)*
Filing system	Any structured set of personal data, which is accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.	Hard copy storage systems. Example: *Personnel file.*

5.8.3 Data protection principles

5.8.3.1 General

We will process personal data in accordance with the following principles as laid down in applicable privacy and data protection law.

5.8.3.2 The principles

Principle 1: Lawful, fair and transparent

Fair: We shall refrain from processing personal data in a manner that is unduly detrimental, unexpected or misleading to the individuals concerned.

Transparent: We shall be clear, open and honest with data subjects regarding why and how it processes personal data.

Lawful: We shall ensure that all processing of personal data has a legal basis.

Principle 2: Purpose limitation

We will only process personal data for specified, explicit and legitimate purposes.

Specified and explicit: We will identify the purpose for each processing activity.

Legitimate: The purpose must be justified with respect to our business.

We will not process personal data for purposes that are incompatible with the purpose for which the personal data was collected. In order to do so, we will adopt the following approach:

- We will establish appropriate measures to prevent easy extraction of personal data from one system to another, unless the two systems are meant to exchange data.
- We will identify, to the extent possible, the data source to determine whether the data was originally collected for another purpose.
- If the data was originally collected for another purpose, we will perform a compatibility test, based on the following criteria:

Criteria	Description
Link	The closer the link between the original and the new purpose, the more likely it is that the new purpose is compatible.
Context	If the context of the original purpose and the new purpose is similar, the more likely it is that the new purpose is compatible.
Nature	The less private/personal the data is, the more likely it is that the new purpose is compatible.
Expectation	If the new purpose is generally expected, or if we, prior to the original processing, have informed about the possibility that the data may be used for a subsequent purpose, the more likely it is that the new purpose is compatible.

Consequences	If the processing for the new purpose does not adversely affect the data subjects, the more likely it is the new purpose is compatible.
Safeguards	If appropriate safeguards, such as encryption or pseudonymisation, are implemented when data is being processed for new purposes, the more likely it is that the new purpose is compatible.

Subject to the test explained above, these purposes would typically be compatible: Audits, business controls, investigations, reporting; Dispute resolution; Legal and business affairs; Archiving, statistics and bookkeeping; Insurance.

We may process anonymous data for subsequent purposes without restrictions, as this is no longer personal data.

Principle 3: Data minimization

We will only process personal data that is relevant and necessary for the purpose, and will:

- Identify the types of personal data processed, to assess the necessity of the data.
- Encourage personnel to avoid the use of identifiers (if practically possible) and to limit the amount of personal data in documents and forms, whether electronic or in hard copy.

Principle 4: Data accuracy

We will take appropriate measures to ensure that personal data is accurate, complete and, where necessary, up-to-date. To achieve this, we will:

- implement appropriate routines when collecting personal data to ensure the accuracy of the data input.
- implement appropriate routines for periodic or ad-hoc reviews of systems and documents containing personal data that requires maintenance to ensure that the data is kept up-to-date.
- implement appropriate routines to allow the data subjects to request, or enable them to carry out, the correction, completion and updating of personal data of themselves.

Principle 5: Storage limitation

We will not retain personal data for longer than necessary for the purpose for which it was collected. To achieve this, we will:

- identify the envisaged retention periods (when personal data must be deleted), including the reason for the retention period.
- implement automatic deletion routines to the extent reasonably possible.

- if the deletion routines are manual, implement tasks, notices or other mechanisms to ensure that the routines are adhered to.
- encourage the use of systems/platforms for archiving and communication, to limit unstructured data.
- if personal data is stored for latent purposes (such as to defend potential claims), but is otherwise not needed for day-to-day operations, appropriate measures will be taken to limit data access and prevent the use of the data in day-to-day operations (blocking or limited processing/access). If reasonably possible, such archived data should preferably be pseudonymised (de-identified, such as by replacing the name/identifier with an ID).
- ensure that any processor processing data on behalf of us are obliged to return or delete personal data upon our instruction.
- consider anonymisation as an alternative to deletion if the data may continue to serve a purpose in anonymised form. Anonymisation means that the data is unlikely to be re-identified by reasonable means.

- if system limitations make it necessary to retain data in backup after the expiry of the data retention period, we will ensure that the data in backup is subject to strict access control and that it is not used operationally.

Principle 6: Integrity and confidentiality

We will ensure the appropriate security of the personal data as further described below.

5.8.4 Legal basis

5.8.4.1 General

We shall identify the applicable legal basis for each processing activity. If no legal basis is identified as applicable, the processing activity must be amended or terminated.

5.8.4.2 Regular personal data

For processing of personal data that are not special categories of personal data (non-sensitive personal data), we may rely on any of the following legal bases under the GDPR article 6:

Legal bases	Description	Requirement	Examples of purposes
Agreement	The data processing is necessary to fulfil an agreement with the data subject, or to take steps prior to entering into such agreement.	The agreement must be with the data subject. This legal basis cannot be relied upon if the agreement is with business partners (legal entities).	• Recruitment • HR.

Legitimate interests	**The data processing is necessary in order to achieve a legitimate interest, unless such interest is overridden by the rights and interest of the data subjects.**	**The legitimate interest of us or a third party (such as a business partner) is identified; the data is necessary to achieve the interest; and, after a balancing of interests, the legitimate interest outweighs the rights and interests of the data subject.**	• **Contract management with business partners** • **Mergers and acquisitions** • **HR administration**
Legal obligation	The data processing is necessary to comply with a legal obligation laid down in EU/EEA member state law.	The legal obligation must be laid down in EU/EEA member state law, explicitly or implicitly.	• Ethics helpline • Bookkeeping • Safety and security
Vital interest	**The data processing is necessary to protect the vital interests of the data subject**	**"Life-or-death" scenarios,**	• Emergency response
Public interest	**The data processing is necessary for the performance of tasks carried out by a public authority or private organization acting in the public interest.**	**Exercise of official authority.**	• Public information
Consent	The data subject has consented to the processing.	The consent must be given in accordance with GDPR art. 7.	• Use of employee images on the intranet or the internet • Retention of data of non-selected job candidates after the recruitment process has been completed

5.8.4.3 Special categories of data (sensitive data)

For special categories of data (sensitive data), we must in addition have a legal basis pursuant to GDPR article 9. Sensitive data are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation).

For processing of such sensitive personal data, we may rely on any of the following legal bases:

Legal bases	Description	Requirement	Examples of purposes
Employment	The data processing is necessary for the purposes of carrying out obligations and exercising specific rights in the field of employment and social security and social protection law.	Must be permitted by law in each EU/EEA member country.	• Sick leave management. • Workplace facilitation due to health issues. • Alcohol or drug tests at the workplace if required for security reasons.
Vital interest	**The data processing is necessary to protect the vital interests of the data subject where the data subject is incapable of giving consent.**	**"Life-or-death" scenarios**	• Emergency response.
Public data	**The data processing relates to personal data which are manifestly made public by the data subject**	**The data subject him/herself must obviously have made the data public.**	• Public relations (such as to process a political party affiliation that a person has made public).
Legal claims	The data processing is necessary for the	The claim may be founded in law, in	• Litigation (civil or criminal).

	establishment, exercise or defense of legal claims.	contract or otherwise.	• Responding to binding subpoenas from public authorities.
Consent	The data subject has explicit consented to the processing.	The consent must be given in accordance with GDPR art. 7.	• Access control.

5.8.4.4 Consents

When relying on consents, we will ensure that the following conditions are adhered to:

Conditions	Description
Freely given	The consent must be voluntary. It must be as easy to say no as to say yes, without detriment.
Specific	The consent must be specific to one single purpose.
Informed	The consent text must explain the subject matter and to which entity the consent is given.
Unambiguous	The consent must be given by an affirmative act (opt-in).
Demonstrated	The consent must be documented (electronically or in hard copy)
Balance	Consents cannot be relied upon if there is a clear imbalance between us and the data subject. As a rule, we will not rely on consents from employees, with the exception of extraordinary circumstances where it is obvious that the choice of the employee is voluntary.

5.8.4.5 Criminal offences and convictions

We may process personal data relating to criminal offences and convictions only if it has a legal basis, either consent, vital *interest* or *legal claims*, as described above.

Criminal conviction data is data relating to individuals sentenced to jail, fines or other criminal sanctions by courts of law (or similar competent institutions), as well as questions and answers about whether or not an individual has a criminal record. Criminal offence data is data relating to criminal allegations or proceedings.

5.8.4.6 Unique identifiers

We may only process social security numbers and other unique identifiers when there is a justified need for certain identification and the method is necessary to achieve such identification. We will not process social security numbers and other unique identifiers for authentication purposes.

5.8.5 Transparency

5.8.5.1 General

We will be transparent about our data processing operations by providing the data subjects with appropriate privacy information.

5.8.5.2 Content of the privacy information

We will inform the data subjects of why and how their data is processed, as required pursuant to GDPR article 13 and 14. The information shall be in a clear and plain

language. The privacy information shall be reviewed periodically in order to ensure that it is kept up-to-date.

5.8.5.3 Communication of the privacy information

We will ensure that the privacy information are easily accessible, such as by communicating them in our agreements or on our website. We shall also provide relevant privacy information upon a data subject's request.

If we develop (on our own or through service providers) software, platforms or other solutions for the data subjects' use, we will consider incorporating specific privacy information in such solutions to facilitate privacy by design. This could be information given in apps, on websites, or on psychical signs.

5.8.5.4 Data subject rights

We will respect the data subjects' rights, including the right to data access, rectification, erasure, restriction, portability and objection. However, we will ensure that the qualifying conditions have been met, and that the limitations to these rights are observed.

5.8.5.5 Automated decision-making

We may use automated decision-making, including profiling, which produces legal effects on, or similarly affects, the data subjects. An example is automated assessments of job applications in recruitment. For such decision-making, we will fulfil the requirements of GDPR article 22.

5.8.5.6 Marketing

We may perform limited marketing activities. We may send direct marketing by e-mail only to the following recipients: those who have consented, or to those who are existing business partners. The recipients will be given the opportunity to opt-out to future e-mail marketing.

5.8.5.7 Privacy by design and privacy by default

If we develop (on our own or through service providers) software, platforms or other solutions, we will implement appropriate measures designed to implement data protection principles as an integrated feature of the solutions. We will configure such solutions so that they, by default, limit the amount of personal data, the extent of the data processing and the period of retention to a minimum.

5.8.5.8 Joint control

Joint control exists when two or more controllers jointly determine the purposes and means of processing, either intra-group or with respect to external business partners.

Where we (as controllers) cooperates with one or more other controllers (affiliate or external entity) with respect to processing of personal data, a case-by-case assessment will be made of whether they act as joint controllers. As a starting point for such assessment, we will consider joint control likely if the parties pursue the same overall goals and they contribute to the each other's data processing.

If we conclude that joint control exists, a joint controller agreement shall be concluded. Such agreement shall determine the parties' respective responsibilities for compliance with applicable laws and regulations, including the duty to provide privacy information to data subjects and the roles and responsibilities vis-à-vis the data subjects with respect to handling data subjects' rights requests.

5.8.6 Transfer to countries outside the EU/EEA

All the countries within the EU/EEA region have implemented the GDPR and thus ensured that personal data are handled properly.

In order to transfer or process personal data outside of the EU/EEA, an adequate level of protection must be ensured. This can be ensured by entering into standard privacy regulations adopted by the European Commission (Standard Contractual Clauses).

If the transfer is made to the US, Privacy Shield shall apply if available. If the Company is to use the Privacy Shield, the Company shall verify that the recipient is listed; assess whether the transfer is in accordance with the principles of processing personal data; and conduct a risk assessment.

5.8.7 Processors and DPAS

5.8.7.1 General

When engaging processors, we will use the following four-step approach:

Step 1: Determination of roles

Firstly, we shall determine whether the entity in question acts as a processor. A processor is a company that processes personal data on behalf of us without independently determining why the processing takes place, what data should be processed and how long the data is to be retained.

Step 2: Vetting

Prior to engaging a processor, we will verify that the processor provides sufficient guarantees to meet the requirements of applicable data protection law. We may do so by requesting relevant privacy documentation and information in a procurement process, or by other appropriate means.

Step 3: Concluding a DPA

We will conclude a data processing agreement / information management agreement (DPA/IMA, hereinafter referred to as "DPA") with each processor. A DPA may form an appendix to another agreement (such as a services agreement).

As a main rule, we will use our template DPA. If the processor insists on using its own DPA template, and we are not in a position to require the use of our template, the processor's template shall be reviewed to ensure that it fulfils the requirements of applicable laws and our standards.

Step 4: Auditing

We will verify compliance with the DPAs.

Any DPA shall contain the right for us to audit the processor.

We may request the processor to regularly prepare data security reports. We will review the report(s) and assess the adequacy of the data security and privacy measures. If the report reveals red flags, we shall request further information. If we have reason to believe that the data security or privacy standards of the processor is inadequate, a more thorough audit shall be performed, such as an on-site audit. If we are dissatisfied with the level of data security or privacy standards, we shall terminate the DPA (if the DPA allows such termination).

5.8.8 Data sharing with independent controllers

Whenever we, as controller, shares personal data with another separate controller, we will consider formalising this by an agreement to protect the personal data against unlawful processing.

Whenever we, as controller, receives personal data from another separate controller, we will consider imposing a contractual obligation on such controller to notify the data

subjects of the fact that we are a recipient of the personal data, to encourage such controller's compliance with the GDPR article 13.

5.8.9 Records of processing activities

We shall establish records of processing activities. The purpose of such records is to comply with the GDPR article 30 and to facilitate compliance with other GDPR requirements. When establishing records of processing activities, the Norwegian Supervisory Authority's template shall be used.

It is the responsibility of each data processing owner to complete and maintain such records. The data processing owner is the role that has the functional responsibility, such as the project responsible.

The records shall be revised periodically. It should also be updated if changes are made to the operation to which it relates.

5.8.10 Data security

We will implement and maintain appropriate technical and organisational measures to ensure an appropriate level of data security to prevent accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

For data that constitutes personal data, we will ensure that its data security measures take due consideration to the following aspects:

Security criteria	Definition	Description/examples
Confidentiality	Protection against unauthorised access or disclosure of data.	1. Employees and business partners will be subject to adequate confidentiality obligations. 2. Databases will be encrypted and subject to adequate access control. 3. Agreements with IT vendors will include data security obligations. 4. Physical facilities will be adequately protected against unauthorised access.
Integrity	Protection against unauthorised amendments to or deletion of data.	1. Databases will be encrypted and subject to adequate access control. 2. Key documents will have version control (revision history).

Accessibility	Access to data when needed.	1. Agreements with key IT service providers will have adequate SLAs. 2. Material data will be remotely accessible (VPN or similar).
Resilience	Business continuity is ensured	1. Agreements with key IT service providers will have adequate SLAs. 2. Data will be backed up.

[3] The template (in Norwegian) can be found at: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/protokoll-over-behandlingsaktiviteter/

5.8.11 Data breach handling

We may potentially experience a personal data breach – a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. If this happens, we shall within 72 hours assess whether we have to inform the data subjects and/or the relevant data protection authority.

Employees who suspect or detect unwanted incidents related to the processing of personal data shall immediately report the incident to their immediate superior or Human Resources manager. Human Resources manager is responsible for informing the relevant data protection authority.

5.8.12 Privacy risk assessment

We will periodically perform a general privacy risk assessment of our business. The purpose of such assessment is to identify potential privacy risks and to identify measures apt to minimize such risks. In the context of privacy, risks (the undesired consequences of an event) are particularly: Physical damage; Discrimination; Identity theft; Fraud; Financial loss; Damage to reputation; Economic or social disadvantage; Unauthorised disclosure of or access to special categories of data; Unauthorised disclosure of or access to data concerning personal aspects, such as economic situation or evaluation of performance at work.

The risk assessment should at least account for: (i) level of acceptable risk, (ii) potential unwanted events, (iii) the likelihood of these events occurring, (iv) the privacy consequence if the event occurs, and (iv), if the risk is unacceptable, measures to address the risk.

5.8.13 Data protection impact assessment

Where a processing operation, such as the use of new technology, is likely to result in a high privacy risk, taking into account its nature, scope, context and purpose, we will perform a data protection impact assessment (DPIA).

A DPIA must at least contain (i) a systematic description of the envisaged processing operation, (ii) an assessment of its necessity and proportionality, (iii) an assessment of privacy risks, and (iv) measures to address the risks.

5.8.14 Identifying lead supervisory authority

If communication with a supervisory authority is required with respect to *cross border data processing* that includes more than one EEA country, the lead supervisory authority shall be identified.

The supervisory authority is the authority of the country in which our main establishment is located. The main establishment is located at the place of our central administration, unless the decisions relating to the purposes and means of the

processing are made in another establishment, which has the power to implement such decisions.

5.8.15 Training

We will provide data protection and privacy training to our personnel.

Personnel with permanent or regular access to personal data, involved in the collection of personal data or in the development of tools used to process personal data, shall complete mandatory privacy and data protection training. Relevant personnel should be defined according to their exposure to processing of personal data in their position and daily tasks. In particular, relevant personnel are:

- People and Leadership (Human Resources) function, including the business area HR and shared HR services
- Procurement function, more specifically IT procurement and personnel handling information relating to temporary agency workers and contractors.
- Safety function, more specifically personnel within Health and working environment, personnel handling security incidents involving identified individuals and personnel emergency response teams
- Legal function
- Corporate Audit
- IT function, more specifically personnel dedicated to information security, applications support and other cross-group IT services
- Line managers

5.9 Appendix 9; Personal Trading Policy

5.9.1 Purpose

The purpose of this policy is to prevent staff members' own-account trading from constituting an actual or potential conflict of interest with the company or the company's external parties.

The policy also seeks to ensure that there is no own-account trading which may raise doubts as to whether an employee has misused inside information or other confidential information, or which may harm the reputation of the Company.

The HR manager is responsible for the implementation and monitoring of personal trading policy

5.9.2 Personal transactions

5.9.2.1 Introduction

This policy contains restrictions on own-account trading for you as a staff member in the Company.

Own-account trading also includes trading conducted for the account of related parties. Related parties means;

(i) Spouse or person with whom the staff member is living in a marriage-like relationship (such as cohabitant, registered partner),
(ii) Dependent children of the staff member, and dependent children of a person as mentioned in (i),
(iii) A company in which the staff member or someone mentioned in (i), (ii) or (iv) has a controlling interest as defined in the Norwegian Private Limited Liability Companies Act section 1-3 second paragraph, the Norwegian Public Limited Liability Companies Act section 1-3 second paragraph, or the Norwegian Partnerships Act section 1-2 second paragraph,
(iv) Any person with whom it must be assumed the staff member has binding cooperation with respect to the exercise of rights as a holder of a financial instrument.

5.9.2.2 Limitations, exceptions and discretionary exemptions

You shall not engage in own-account trading in;

(i) Debt or equity instruments ("**Instruments**") issued by companies in segments within the Company's investment strategy or potential business partners.
(ii) Derivative agreements with instruments as mentioned in (i) as underlying.

The prohibition does not apply where such a transaction is carried out by a fund manager on behalf of you, and in accordance with current authorisation to discretionary mandate, and without it being given orders/instructions about such investment, or in a fund where you are an investor.

However, the staff member may not give an active management mandate which is mainly aimed at investments as stated in section 2.2.

5.9.2.3 [Optional: Existing investments in violation of the regulations

Staff members, who at the time of joining the Company have investment that are in violation of the above limitations, must divest the investments within [12 months].

The CEO may under special circumstances, extend the deadline or agree to alternative solution]]

5.9.2.4 General checklist

These general principles apply for all own account trading:

(i) All trading must be in accordance with applicable laws.

(ii) Conflict of interest between the Company and the staff member shall be avoided. You shall always put the Company's interests before your own interests.

5.10 Appendix 10; Payment Procedure

5.10.1 Introduction

This procedure describes the guidelines all employees must follow to comply with the Company's fraud prevention objective.

It should be read in conjunction with the company's Cyber Security Policy as fraud is frequently a result of data hacking:

- By "social engineering" hackers may obtain access by deceiving the user. The hacker often uses charm to obtain sensitive information he otherwise would not have had access to.
- By "phishing" hackers send e-mails that look like e-mails from recognised sources. The intention is to steal sensitive data, for example credit card or log-in information.

Our overall ambition is to act in a manner that reduces the danger of the company suffering from embezzlement (internal risk) and fraud (external risk).

Effective control over expenditures must be maintained at all stages and supported by an appropriate accounting system. Clear payment procedures give guidance on the basic principles and safeguards associated with authorizing expenditures and making payments. Supported by an appropriate accounting system, they can reduce misappropriation of funds, theft of inventory, and petty corruption.

5.10.2 Control environment

Expenditures should be authorised with due consideration to separation of duties. No individual should be able to control all aspects of the payment authorization procedure, and different people should be responsible for ordering goods and services, for approving payments, and for processing payments.

Authorizations in our online bank(s) shall be granted jointly by two administrators. The authorizations shall be listed in– "Chart of Accounts and Approval Matrix - Online Bank". The "four eyes principle" reduces unnecessary room for both malpractice and costly mistakes, and reduces the likelihood of illicit behavior.

The Company's bank(s) shall be instructed to align the administrator profile in the online bank in accordance with the approval matrix. The Company shall, if possible, annually verify compliance with this procedure by obtaining an online bank report evidencing such compliance with the procedure.

In the following circumstances, manual confirmation by phone shall always be made in accordance with the checklist:

- When receiving payment instructions from new persons or new email addresses (sender's email shall always be scrutinized with care).
- When receiving instructions to effectuate payments to – or register – new vendor accounts.
- When receiving instructions to effectuate payments to new bank account numbers for a known vendor account.
- Prior to effectuating payments exceeding NOK 3 000 000.
- Prior to acting in accordance with emails from CEO or other executive management.

Example 1 – "CEO Fraud"

Fraudsters send an email to an employee and make it look like the e-mail is sent by the CEO or another senior position in the Company. Such an email may ask for an urgent and strictly confidential payment to be made.

To assess if a payment request is a fraud attempt the receiver of such a request may:

- Hold the cursor over the link to verify the e-mail address.
- Respond by separate e-mail (not by replying to the received e-mail), to the person requesting payment.
- Phone the CEO or the person requesting payment, to verify the identity.

Example 2 – Invoice Fraud

Fraudsters contact an employee and pose as one of the Company's suppliers and they ask that future payments are sent to a different bank account. The fraudster may send the new details (sometimes on headed note paper) advising of changes to the supplier's bank account.

Contact the supplier by telephone (via the number listed in the contract documents - not the number on the notice) and verify.

Standardized and harmonized practices build up transparency, which makes spotting and preventing payment fraud easier. In addition, it is easier to control the risk related to data transfer and system management:

- Eliminating manual phases through automation of the payment process and focus on end-to-end safety reduces both the risk of fraud and the risk of mistakes.
- If possible, authorization for payments should be separated from the process of executing payments, with appropriate validation and recording at each step.

- Double approval of changes made in the vendor master data, as well as user rights shall always be applied.
- System access to make and authorize changes should be restricted and password protected.
- It must be ensured that signature authorizations are cancelled or changed properly in connection with staff rotation, internal moves etc.

5.10.3 Checklist – payment execution

The following check list contains key principles to be considered in connection with payment execution:

- Payments shall in general be supported by a purchase order, as well as an invoice or other documentation properly approved in accordance with our procedures.
- Any increase in cost over the order price must have been agreed upon. No employee shall be positioned to authorize their own or their direct superior's reimbursements.
- An invoice should only be approved for payment if it has a purchase order number or if it is paid to registered suppliers. There should be checks to ensure that the goods or services acquired have been supplied in accordance with the relevant agreement(s) before payment is made.
- The invoice should only be accepted if issued under a legitimate business name, address and bank account number. It is a red flag if the address is residential or a post-office box.
- The invoice must always be arithmetically correct, in accordance with contract or other commitment and properly discounted.
- The invoice must never be a duplicate, nor previously passed for payment.
- Multiple invoices with amounts right under the threshold for requiring an additional review should be subject to further scrutiny.
- Checks for duplicate invoices should be carried out periodically.

5.10.3.1 Chart of Accounts - Online Bank

Accounts:

Account name	Account number	Legal Entity
Eureka Pumps AS - CAD	3185 41 56945	Eureka Pumps AS
Eureka Pumps AS - EUR	3185 15 26563	Eureka Pumps AS
Eureka Pumps AS - GBP	3185 17 23482	Eureka Pumps AS
Eureka Pumps AS - NOK	3201 37 61093	Eureka Pumps AS

Eureka Pumps AS - Skatt - NOK	3201 37 61107	Eureka Pumps AS
Eureka Pumps AS - USD	3185 05 33779	Eureka Pumps AS
Eureka Logistics – EUR	3185 42 32064	Eureka Logistics AS
Eureka Logistics – NOK	3207 33 60667	Eureka Logistics AS
Eureka Logistics – skatt	3207 33 93107	Eureka Logistics AS
Eureka Group AS Driftskonto	3201 49 45597	Eureka Group AS
Eureka Group AS Emisjonskonto	3201 51 98841	Eureka Group AS
Eureka Group AS Skattetrekk	3201 49 45600	Eureka Group AS
Eureka Group II AS Kassekredit	3207 38 05995	Eureka Group II AS
Eureka Group AS II Rammelån	3207 83 46166	Eureka Group II AS

5.10.3.2 Approval Matrix – Online Bank

Name	**Company**	**1st Approver**	**2nd Approver**	**Bank Reconciliation** [Optional]
Tom Munkejord	Eureka Group AS Eureka Group II AS Eureka Pumps AS Eureka Logistics AS	No No	Yes Yes	
Fredrik Aarnes	Eureka Group AS Eureka Group II AS Eureka Pumps AS Eureka Logistics AS	Yes	Yes	
Henning Smith Kristiansen	Eureka Group AS Eureka Group II AS Eureka Pumps AS Eureka Logistics AS	Yes	Yes	
Sissel Skår	Eureka Group AS Eureka Group II AS Eureka Pumps AS Eureka Logistics AS	Yes	No	
Birgitte Weltzin	Eureka Group AS Eureka Group II AS Eureka Pumps AS Eureka Logistics AS	Yes	No	

For all companies;

- ❖ All payments require double approval
- ❖ All payments above NOK 5 000 000 require CEO as second approver (except salaries)

All payments to banks outside Norway require CFO as second approver up to NOK equivalent 5 000 000.

Call-back checklist	Comment	Completed by	Reviewed by
In the following circumstances, manual confirmation by phone shall always be made: • When receiving payment instructions from new persons or new email addresses (sender's email shall always be scrutinized with care). • When receiving instructions to effectuate payments to – or register – new vendor accounts. • When receiving instructions to effectuate payments to new bank account numbers for a known vendor. • Prior to effectuating payments exceeding NOK 5 000 000 • Prior to acting in accordance with emails from CEO or other executive management.			
Call-back required? ☐ Yes ☐ No If Yes, reason for call-back ☐ Payment instructions received from new persons or new email addresses ☐ New vendor account	If no call-back is required, provide reason for this: [...] If we have paid to the same bank account before, please provide reference to the relevant call-back checklist		

Call-back checklist		Comment	Completed by	Reviewed by
☐ Payment exceeding NOK 5 000 000. ☐ Payment made in accordance with email from CEO or other executive management.		Document reference: [..]		
If call-back is required, complete call-back to validate authenticity of payment instruction and bank account details using known (e.g. maintain on systems/static data) or independently verified (e.g. through web search) contact details.				
Contact details obtained from: Bank details confirmed by: Bank details confirmed without deviations: Date and time of call-back: Contact details for the person confirming the bank details:	[Contact list] [.....] [Yes/No] [.....] [.....]	[Insert original source of payment request, including document reference to the actual payment instructions received.]		