1 We are patient and courteous

2 We are inclusive

We welcome and support people of all backgrounds and identities. This includes, but is not limited to members of any sexual orientation, gender identity and expression, race, ethnicity, culture, national origin, social and economic class, educational level, colour, immigration status, sex, age, size, family status, political belief, religion, and mental and physical ability.

3 We are considerate

We all depend on each other to produce the best work we can as a company. Our decisions affect clients and colleagues, and we take those consequences into account when making decisions.

4 We are respectful

We won't all agree all the time, but disagreement is no excuse for disrespectful behaviour. We will all experience frustration from time to time, but we cannot allow that frustration become personal attacks. An environment where people feel uncomfortable or threatened is not a productive or creative one.

5 We choose our words carefully

We always conduct ourselves professionally. We are kind to others. We do not insult or put down others. Harassment and exclusionary behaviour aren't acceptable. This includes, but is not limited to: -

(a) Threats of violence.
(b) Discriminatory jokes and language.
(c) Sharing sexually explicit or violent material via electronic devices or other means.
(e) Personal insults, especially those using racist or sexist terms.
(f) Unwelcome sexual attention.
(g) Advocating for, or encouraging, any of the above behaviour.

6 We do not harass others

If someone asks you to stop something, then stop.

7 When we disagree

We try to understand why. Differences of opinion and disagreements are mostly unavoidable. What is important is that we resolve disagreements and differing views constructively.
Our differences

8 Our differences

Are our strengths. We can find strength in diversity. Different people have different perspectives on issues, and that can be valuable for solving problems or generating new ideas. Being unable to understand why someone holds a viewpoint doesn't mean that they're wrong. Don't forget that we all make mistakes, and blaming each other doesn't get us anywhere.

Instead, we focus on resolving issues and learning from mistakes

1 Scope of the Policy

This Policy Document encompasses all aspects of security surrounding confidential company information and client information. It must be distributed to all company employees. All company employees must read this document fully and understand this policy in its entirety. This document will be reviewed and updated by Management on a triennial basis or when relevant to include newly developed security standards into the policy and distribute it all employees and contracts as applicable.

2 Information Security Policy

ABCconsulting handles sensitive client and customer information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect privacy, to ensure compliance with various regulations and to guard the future of the organisation. ABCconsulting commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end management are committed to maintaining a secure environment in which to process information so that we can meet these promises.

Employees handling sensitive data should ensure:

(a) Handle Company and client information in a manner that fits with their sensitivity.
(b) Limit personal use of the Company information and telecommunication systems and ensure it doesn't interfere with your job performance.
(c) The Company reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose.
(d) Do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal.
(e) Do not disclose personnel information unless authorised.
(f) Protect sensitive information.
(g) Keep passwords and accounts secure.
(h) Request approval from management prior to establishing any new software or hardware, third party connections, etc.
(i) Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval.
(j) Always leave desks clear of sensitive data and lock computer screens when unattended.
(k) Information security incidents must be reported, without delay, to the legal owner of ABCconsulting, Alan Cardew or the Managing Partner, Beverley Cardew

We each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from the legal owner of ABCconsulting, Alan Cardew or the Managing Partner, Beverley Cardew.

2 Acceptable Use Policy

The Management's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to the ABCconsulting established culture of openness, trust and integrity. Management is committed to protecting the employees, partners and the Company from illegal or damaging actions by individuals, either knowingly or unknowingly.

(a) Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
(b) Employees should ensure that they have appropriate credentials and are authenticated for the use of technologies.
(c) Employees should take all necessary steps to prevent unauthorised access to confidential data.
(d) Employees should ensure that technologies should be used and setup in acceptable network locations.
(e) Keep passwords secure and not share accounts.
(f) Authorised users are responsible for the security of their passwords and accounts.
(g) All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature.
(h) Because information contained on portable computers is especially vulnerable, special care should be exercised.
(h) Postings by employees from a Company email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Company, unless authorised to do so.
(i) Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

3 Disposal of Stored Data

All data must be securely disposed of when no longer required by the Company, regardless of the media or application type on which it is stored.

An automatic process must exist to permanently delete on-line data, when no longer required.

The Company will have procedures for the destruction of hardcopy (paper) materials. These will require that all hardcopy materials are crosscut shredded so they cannot be reconstructed.

The Company will have documented procedures for the destruction of electronic media. These will require:

(a) All data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped.
(b) If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion.

4 Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

(a) All information, applications, and infrastructure components are appropriately secured to prevent unauthorized access, use, disclosure, modification, damage or loss of data.
(b) Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day company practice.
(c) Distribute this security policy document to all company employees to read.
(d) Company security policies must be reviewed triennially and updated as needed.

5 System and Password Policy

All users, including contractors and vendors with access to the Company systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

(a) A system configuration standard must be developed along industry acceptable hardening standards.
(b) System configurations should be updated as new issues are identified.
(c) System configurations must include common security parameter settings.
(d) The systems configuration standard should be applied to any new systems configured.
(e) All vendor default accounts and passwords for the systems have to be changed at the time of provisioning the system/device into the Company network and all unnecessary services and user/system accounts have to be disabled.
(f) All unnecessary default accounts must be removed or disabled before installing a system on the network.
(g) Security parameter settings must me set appropriately on System components.
(h) All unnecessary functionality (scripts, drivers, features, subsystems, file systems, web servers etc.,) must be removed.
(i) All unnecessary services, protocols, daemons etc., should be disabled if not in use by the system.
(j) Any insecure protocols, daemons, services in use must be documented and justified.
(k) All user must use a password to access the company network or any other electronic resources.
(l) All user ID's for terminated users must be deactivated or removed immediately.
(m) The User ID will be locked out if there are more than 5 unsuccessful attempts. This locked account can only be enabled by the system administrator. Locked out user accounts will be disabled until the administrator enables the account.
(n) Group, shared or generic user account or password or other authentication methods must not be used to administer any system components.
(o) All non-console administrative access will use SSL before the administrator password is requested.
(p) System services and parameters will be configured to prevent the use of insecure technologies like telnet and other insecure remote login commands.
(q) Administrator access to web based management interfaces is encrypted using strong cryptography.
(r) The responsibility of selecting a password that is hard to guess generally falls to users. A strong password must:
- Be as long as possible (min of 8 characters include numbers and special characters).
- Include mixed-case letters, if possible.
- Include digits and punctuation marks, if possible.
- Not be based on any personal information.
- Not be based on any dictionary word, in any language.

5 Anti Virus Policy

(a) All machines must be configured to run the latest anti-virus software as approved by the Company. The preferred application to use is Kaspersky Anti-Virus software, which must be configured to retrieve the latest updates to the antiviral program automatically on a daily basis. The antivirus should have periodic scanning enabled for all the systems.

(b) The antivirus software in use should be cable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits)
(c) Removable media (for example USB and others) not be used.
(d) All the logs generated from the antivirus solutions have to be retained as per legal/regulatory/requirements (6 months)
(e) Master Installations of the Antivirus software should be setup for automatic updates and periodic scans.
(f) End users must not be able to modify and any settings or alter the antivirus software
(g) E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus.

5 Patch Management Policy

(a) All Workstations, servers, software, system components etc. owned by the Company must have up-to-date system security patches installed to protect the asset from known vulnerabilities.
(b) Wherever possible, all systems, software must have automatic updates enabled for system patches released from their respective vendors.
(c) Any exceptions to this process have to be documented.

6 Remote Access Policy

Remote access privileges are not permitted for any employee, freelance consultants or anyone associated with ABCconsulting.

7 Responsibilities

Any concerns relating to a breach of the Policy should be reported directly and immediately on discovery (if possible) to:

Alan Cardew Legal owner of ABCconsulting
Beverley Cardew Managing partner of ABCconsulting

8 Communication and Review

This policy will be communicated to all employees during induction, and at staff meetings. This policy will be reviewed on a triennial basis or when a material change in law dictates.

Data protection policy of ABCconsulting

Context and overview

Key details:

- Policy prepared by: Alan Cardew
- Approved by management on: 10.05.2018
- Policy became operational on: 18.05.2018
- Policy modified on: 10.10.2019

Introduction

ABCconsulting in the course of its business needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees, government agencies and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and to comply with the law.

Why this policy exists

This data protection policy ensures that ABCconsulting:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

The EU Data Protection Regulation (GDPR)

The GDPR describes how organisations including ABCconsulting must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR is underpinned by important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways

8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of ABCconsulting
- All branches of ABCconsulting
- All staff and volunteers of ABCconsulting
- All contractors, suppliers and other people working on behalf of ABCconsulting

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act.

This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- plus any other personal information relating to individuals

Data protection risks

This policy helps to protect ABCconsulting from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with ABCconsulting has some responsibility for ensuring data is collected, stored and handled appropriately.

Everyone who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The managing partners and owners, Alan & Beverley Cardew are ultimately responsible for ensuring that ABCconsulting meets its legal obligations.

- The data protection officer is Alan Cardew and is responsible for:

    a. Keeping all staff, volunteers, contractors, suppliers and other people working on behalf of ABCconsulting aware about data protection responsibilities, risks and issues.
    b. Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    c. Arranging data protection training and advice for the people covered by this policy.
    d. Handling data protection questions from staff and anyone else covered by this policy.
    e. Dealing with requests from individuals to see the data ABCconsulting holds about them (also called 'subject access requests').
    f. Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
    g. Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    h. Performing regular checks and scans to ensure security hardware and software is functioning properly.
    i. Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
    j. Approving any data protection statements attached to communications such as emails and letters.
    k. Addressing any data protection queries from journalists or media outlets like newspapers.
    l. Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, staff, volunteers, contractors, suppliers and other people working on behalf of ABCconsulting can request it from the managing partners of ABCconsulting.
- ABCconsulting will provide internal training to all staff to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Company staff should request help from the managing partners of ABCconsulting if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the managing partners of ABCconsulting.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a secure location.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- Sensitive data should never be stored on removable media (such as a USB Stick, CD or DVD).Data should only be stored on designated drives and servers, and never be uploaded to cloud computing services.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to ABCconsulting unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally.
- Data must be encrypted before being transferred electronically. The managing partners can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area unless that country or territory also ensures an adequate level of data protection.
- Staff should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data accuracy

The law requires ABCconsulting to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort ABCconsulting should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- ABCconsulting will make it easy for data subjects to update the information ABCconsulting holds about them.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by ABCconsulting are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the managing partners (info@abcconsulting.biz).

The managing partners will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, ABCconsulting will disclose the requested data. However, the managing partners will ensure the request is legitimate, seeking assistance from the company's legal advisers where necessary.

Providing information

ABCconsulting aims to ensure that all individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

1 Scope of the Policy

ABCconsulting will do all it can to prevent the company and its employees being exposed to money laundering, to identify the potential areas where it may occur and to comply with all legal and regulatory requirements, especially with regard to the reporting of actual or suspected cases.

2 Definitions

(a) Money laundering is the term used for a number of offences involving the proceeds of crime or terrorism funds. The following acts constitute the act of money laundering:

- Concealing, disguising, converting, transferring criminal property or removing it from Germany.
- Entering into or becoming concerned in an arrangement which is known or suspected of facilitating the acquisition, retention, use or control of criminal property by or on behalf of another person.
- Acquiring, using or possessing criminal property.

These are the primary money laundering offences, and are thus prohibited acts under the legislation. There are two secondary offences:

- Failure to disclose any of these primary offences.
- Tipping off:
  Tipping Off is where someone informs a person or people who are, or who are suspected of being involved in money laundering, in such a way as to reduce the likelihood of their being investigated or prejudicing an investigation. A person found guilty of tipping off or prejudicing an investigation offence is liable to imprisonment a fine or both under the legislation.

3 Policy Statement

This policy refers to the Anti-Money Laundering Law as amended by Article 23 of the Act of 23 June 2017 (Federal Law Gazette 2017 I p. 1822) and replaces Act 7613-2 of 13 August 2008 (Federal Law Gazette 2008 I p. 1690) (GwG 2008) The Act was adopted by the Bundestag with the consent of the Bundesrat as Article 1 of the Act of 23 June 2017 (Federal Law Gazette 2017 I p. 1822). It entered into force on 26 June 2017 in accordance with Article 24 sentence 1 of that Act.

Money Laundering Regulations generally apply to cash transactions in excess of 10,000 Euros. However, Proceeds of Crime Act 2017 (as defined by the 2014/42/EU) applies to all transactions and can include dealings with agents, third parties, property or equipment, cheques, cash or bank transfers.

Key points;

(a) ABCconsulting is committed to the prevention, detection and reporting of money laundering.
(b) All employees must be vigilant for the signs of money laundering.
(c) Any employee who suspects' money laundering activity must report this promptly to the legal owner of ABCconsulting, Alan Cardew or the Managing Partner, Beverley Cardew as the officers delegated to receive such reports.
(d) All payments to ABCconsulting accepted in cash that exceed EUR 10,000 must be reported to the German Financial Intelligence Unit (FIU).

(e) This Policy applies to all employees of ABCconsulting and aims to maintain high standards by preventing criminal activity through money laundering. The Policy sets out the procedures which must be followed to enable ABCconsulting and employees to comply with legal obligations.
(f) This Policy sits alongside the ABCconsulting Anti-Fraud, Bribery and Corruption Policy.
(g) Failure by a member of staff to comply with the procedures set out in this Policy may lead to disciplinary action being taken against them and may also lead to a conviction under Proceeds of Crime Act 2017 and Money Laundering Regulations (BGBl. of 2015, part 1, p. 2025 ff.).
(h) Where ABCconsulting is carrying out regulated activities by way of business then customer due diligence procedures must be followed.
(i) Any member of staff could potentially be caught by the money laundering provisions as noted above, if they suspect money laundering and either become involved with it in some way and/or do nothing about it.
(j) This Policy therefore sets out how any concerns should be raised.
(k) While the risk to ABCconsulting of contravening the legislation is low, it is important that all employees are familiar with their responsibilities. Serious criminal sanctions may be imposed for breaches of the legislation. The key requirement of employees is to promptly report any suspected money laundering activity to the German Financial Intelligence Unit (FIU).

3 Responsibilities

ABCconsulting is committed to implementing risk sensitive policies and procedures relating to customer due diligence, reporting, record keeping, internal control, risk assessment and management, monitoring and management of compliance, along with the communication of policies and processes

Any concerns relating to a breach of the Policy should be reported directly and immediately on discovery (if possible) to:

Alan Cardew Legal owner of ABCconsulting
Beverley Cardew Managing partner of ABCconsulting

4 Reporting

(a) Cash payments to ABCconsulting exceeding EUR1,000 must be reported immediately to the legal owner of ABCconsulting, Alan Cardew or the Managing Partner, Beverley Cardew regardless of whether the employee suspects money laundering activities or not.
(b) All employees must follow any subsequent directions of the legal owner of ABCconsulting, Alan Cardew or the Managing Partner, Beverley Cardew and must not make any further enquiries into the matter. Employees must not disclose or otherwise indicate any suspicions to the person suspected of the money laundering. In addition employees must not discuss the matter with others i.e. colleagues or note on the file that a report has been made in case this results in the suspect becoming aware of the situation.
(c) The legal owner of ABCconsulting, Alan Cardew must promptly evaluate any Disclosure Report, to determine whether it should be reported to the German Financial Intelligence Unit (FIU).
(d) The legal owner of ABCconsulting, Alan Cardew, any employees and freelance consultants will commit a criminal offence if they know or suspect, or have reasonable grounds to do so, through a disclosure being made to them, that another person is engaged in money laundering and they do not disclose this as soon as practicable.

4 Due Dilligence

Customer due diligence means that ABCconsulting must know its clients and understand its business. This is so that ABCconsulting is in a position to know if there is suspicious activity that should be reported.

The 2017 Regulations require that ABCconsulting identifies its customers and verifies the identity on the basis of documents, data or information obtained from a reliable source. Where there is a beneficial owner, who is not the customer then ABCconsulting must identify that person and verify the identity and where the beneficial owner is a trust or similar then ABCconsulting must understand the nature of the control structure of that trust. Finally ABCconsulting must obtain information on the purpose and intended nature of the business relationship.

To determine decide if customer due diligence is necessary three tests are applicable:

Question 1
Is the service a regulated activity? Regulated activity is defined as the provision 'by way of business' of: advice about tax affairs, accounting services, treasury management, investment or other financial services, audit services, legal services, estate agency, services involving the formation, operation or arrangement of a company or trust or dealing in goods or services wherever a transaction involves a cash payment of EUR 10,000 or more.

Question 2
Is the service being provided to a private person, or a customer with its domicile other than Germany?

If the answer to these questions is no then ABCconsulting does not need to carry out customer due diligence.

If the answer to these questions is yes, then ABCconsulting must carry out customer due diligence before any business is undertaken for that client.

Where ABCconsulting needs to carry out customer due diligence then we must seek evidence of identity. For example:

(a) Checking with the customer's website to confirm their business address;
(b) Conducting an on-line search via the relevant authorities to confirm the nature and business of the customer and confirm identities of any directors.
(c) Seeking evidence from the key contacts or Individuals of their personal identity, for example their passport, and position within the organisation.

The requirement for customer due diligence applies immediately for new Customers and should be applied on a risk sensitive basis for existing Customers.

Ongoing customer due diligence must also be carried out during the life of a business relationship but should be proportionate to the risk of money laundering and terrorist funding, based on the other's knowledge of the Customer and a regular scrutiny of the transactions involved.

If, at any time, an employee suspects that a client or customer for whom ABCconsulting is currently, or is planning to carry out a regulated activity, is carrying out money laundering, or terrorist financing, or has lied about their identity then the employee must report this to the legal owner of ABCconsulting, Alan Cardew or the Managing Partner, Beverley Cardew.

In certain circumstance enhanced customer due diligence must be carried out for Example where:

(a) The customer has not been physically present for identification.
(b) The customer is a politically exposed person. Note: A politically exposed person is an individual who at any time in the preceding year has held a prominent public function outside Germany and the EU or international institution/ body, their immediate family members or close associates.
(c) There is a beneficial owner who is not the customer- a beneficial owner is any individual who: holds more than 25% of the shares, voting rights or interest in a company, partnership or trust.

Enhanced customer due diligence could include additional documentation, data or information that will confirm the customer's identity and/or source of the funds to be used in the business relationship/transaction. If ABCconsulting believes that enhanced customer due diligence is required it must consult legal owner of ABCconsulting, Alan Cardew or the Managing Partner, Beverley Cardew prior to carrying it out, to ensure that the checks are completed.

4 Communication and Review

This policy will be communicated to all staff and freelance relocation consultants during induction, and at staff meetings. This policy will be reviewed on a triennial basis or when a material change in law dictates.

1 Scope of the Policy

All ABCconsulting employees and others acting on behalf of ABCconsulting must comply with this Anti-Bribery and Corruption Policy and it extends to all business dealings and transactions in Germany. It is essential that ABCconsulting conducts an effective process of due diligence prior to entering into significant business relationships and that a record is kept of this process.

Any breach of the policy is likely to constitute a serious disciplinary, contractual and criminal matter for the individual concerned. This could constitute gross misconduct for which an offending employee may be dismissed without notice. It may also cause serious damage to the reputation and standing of ABCconsulting.

2 Policy Statement

2.1 Bribery in the public sector

Germany ratified the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions in 1998, by passing the Act on Combating International Bribery, which came into force on 15.02.1999 (BGB of 1998, part II, p. 2327). This Act complemented the provisions in the German Penal Code on bribery in the public sector until the 20.11.2015, when through a new Anti-Corruption law, the Act to Combat Corruption detailed the special regulations regarding both foreign and European public officials were integrated into the general criminal law provisions on corruption (Section 331-335 German Criminal Code). It came into force on 26.11.2015 (BGBl. of 2015, part 1, p. 2025 ff.).

The Criminal Code provides four types of offences of bribery:

(a) Passive bribery (taking bribes) in fulfilling one's public duty (Section 331 of the German Criminal Code).
(b) Passive bribery (taking bribes) as incentive for violating one's duties (Section 332 of the German Criminal Code).
(c) Active bribery (giving bribes) in fulfilling one's public duty (Section 333 of the German Criminal Code).
(d) Active bribery (giving bribes) as incentive for violating of one's duties (Section 334 of the German Criminal Code).

2.1 Bribery in the comercial sector

Section 299 of the German Criminal Code prohibits both active and passive bribery in the private sector regarding employees or agents of a company as recipients of an undue advantage ("for according an unfair preference to another in the competitive purchase of goods or commercial services"). From 30 August 2002 until 25 November 2015, para. 3 of the same provision provided that the offence also applied to commercial bribery carried out abroad (i.e. influencing foreign markets). As of 26 November 2015, the provision has been extended, now also covering the case where an agent or employee of a company, without the consent of his company, performs an act in violation of his duties in the competitive purchase of goods or commercial services. The provision applies equally to the competitive situation both locally and abroad.

ABCconsulting anti-bribery and corruption principles:

(a) We will carry out business fairly, honestly and openly.
(b) We will not give or offer any money, gift, hospitality or other advantage to any person carrying out a business or public role, or to a third party associated with that person, to get them to do something improper.
(c) We will not give or offer any money, gift, hospitality or other advantages to any German or foreign public official with the intention of influencing them to our business advantage.
(d) We will not use intermediaries or contractors for the purpose of committing acts of bribery.´
(e) We will not allow employees or freelance consultants to accept money, gifts, hospitality and other advantages from business associates, actual or potential suppliers, or service providers which are intended to influence a business decision or transaction in some improper way.
(f) Any employee found to be in breach of these principles will face disciplinary action.
(g) Any freelance consultants found to be in breach of these principles will not receive further contacts from ABCconsulting and may face punitive litigation.
(h) No employee will suffer demotion, penalty, or other adverse consequence for refusing to pay bribes, even if it may result in EMEC losing business.
(i) We will avoid doing business with others who do not commit to conducting business without bribery.

3 Responsibilities

Any concerns relating to a breach of the Policy should be reported directly and immediately on discovery (if possible) to:

Alan Cardew Legal owner of ABCconsulting
Beverly Cardew Managing partner of ABCconsulting

4 Communication and review

This policy will be communicated to all staff and freelance relocation consultants during induction, and at staff meetings. This policy will be reviewed on a triennial basis or when a material change in law dictates.