Code of Conduct KBC Group – suppliers' version

1 Scope and purpose

KBC intends to earn, keep and grow trust of all its stakeholders and wants to become the reference in its core markets. In order to maintain and grow this trust it is of utmost importance that we behave responsibly in everything we do, at all layers of the organization. As client centricity is in the heart of our reference strategy, we will also specifically focus on responsible selling and advice. This means we have to go beyond regulation and compliance.

The basic principles are the respect for our customers, colleagues, society and KBC itself, together with our responsive - and our result driven spirit. These are our license to operate. It will guide our behavior and will make us still there tomorrow. The foundation of responsible behavior is integrity, which entails honesty, correctness, transparency and confidentiality, combined with a sound risk awareness."

These principles are the basics for this Code of Conduct and are therefore also binding on all suppliers. This code has to be considered as a minimum set of guidelines, which can be made stricter by local KBC entities, provided that the basic principles set out in this document are not tampered with.

KBC has a right to monitor compliance with the code of conduct. Failure to comply with any of the standards as set out in this code of conduct may lead – after an unbiased assessment – to the termination of the contract.

2 Compliance with rules

KBC expects that supplier's staff observe all legal and internal regulations, like this code of conduct, and has a right to monitor that compliance.

3 Money Laundering & Terrorist Financing

Money laundering and terrorist financing are crimes, and KBC has a statutory duty to combat these practices. The supplier's staff shall not, in any way, get involved in money laundering or terrorist financing. If in doubt, supplier's staff are required to contact the compliance department.

4 Tax laws and regulations

KBC is a responsible taxpayer, basing itself on professionally executed compliance with tax laws and legitimate tax planning, supported by valid business objectives. Consequently, customers may never be given advice of a nature that might prompt them to violate tax laws or regulations. Mechanisms may not be set up that are contrary to standard practice and that clearly aim to promote or result in tax fraud by customers. Additionally, no assistance may be provided in any operations of which the purpose is to procure an unlawful tax benefit for the customer.

5 Data Protection & confidential information

KBC's relationship with customers is based on trust and confidentiality. The conduct of KBC's business is in part determined by the protection of confidential internal customer information, and decisions should be made on the basis of complete and correct data. All information relating to KBC's customers or business partners that Supplier would gain access to, shall therefore be treated as confidential information, and must be processed in accordance with applicable data protection legislation (such as Directive 95/46/EC and its national implementations). All internal information concerning customers and business partners shall be protected from unauthorised usage, disclosure, alteration or destruction.

That information may be used only for the (professional) purpose for which it has been collected. The protection of confidential information applies to all data carriers, regardless of their form.

At no time may any false or biased data be entered into the KBC information systems or information be withheld that is required for decision-making purposes. Unauthorised persons may never be enabled to use the authorisations or technical means given to staff to access KBC company premises or information systems. In all matters, the legal and internal regulations relating to the confidentiality, handling and processing of personal data must be observed.

6 Protection of investors and capital markets

In all financial markets, market abuse – *i.e.* abuse of insider information and market manipulation (price manipulation, diffusion of false information) – is one of the most serious offences against trading ethics. Trading based on confidential information obtained through KBC or on transactions involving a conflict of interests is not permitted. For the same reason, Supplier cannot carry out activities that distort the market price of negotiable financial instruments, or increase their trading volume artificially in order to mislead market participants.

All confidential internal information relating to the KBC group, customers or business partners that Suppliers has become privy to in the course of their work must be protected, and may not be used for personal benefit or the benefit of others.

7 Ethics & Fraud

Responsible behavior is of the utmost importance for KBC. It is important to communicate openly regarding possible mistakes, so that worse mistakes can be prevented and other colleagues can learn from it. Behaviour in the workplace may not inconvenience other staff or jeopardize their health and safety.

In accordance with the KBC Ethics & Fraud Policy, we apply a zero-tolerance policy regarding fraud. The supplier's staff members are required to:

- act honestly and with integrity at all times;
- know and comply with all applicable laws, regulations, internal policies and good business practices applicable to their business and work;
- safeguard the resources for which they are responsible;
- co-operate with and assist, to the fullest extent possible, investigating authorities.

KBC expects the staff to understand the need for internal and external checks and to try not to circumvent them.

It is strictly prohibited, also for Supplier's staff to:

- exert any inappropriate pressure or influence;
- make hurtful remarks;
- act in a way that undermines the integrity or dignity of KBC colleagues;
- conspire against colleagues;
- bullying, harassing or sexually harassing colleagues
- abuse their position on dealings with colleagues

8 Gifts/bribes & other types of corruption

KBC attaches great importance to the avoidance of conflicts of interest; to the transparency of relationships between staff, customers and third parties and, in particular, to the integrity of its staff.

KBC will therefore reject all forms of bribery and corruption, to which KBC applies a zero-tolerance policy.

Bribes can never be offered or solicited or mediated for. Corruption is always considered a breaking point. Should KBC become aware of it, the business relationship with Supplier will be frozen and an in depth investigation is carried out, which may not only lead to mandatory changes at the side of the supplier, but also to a contract cancellation.

KBC wants to avoid that any of its employees who are in contact with suppliers, or who can influence KBC's purchasing decisions, would find themselves in a position of direct or indirect dependence on a supplier. Suppliers therefore shall refrain from offering gifts or entertainment to KBC employees (or, indirectly, to their relatives) in violation of the rules described below. A maximum of 250 EUR applies for all gifts and entertainment offers, calculated per KBC employee, per year, per supplier and on the sum of the value of both offered and received gifts. This policy is also subject to the following limitations:

- cash or equivalents (such as vouchers or financial instruments) are only allowed if donated to charity organisations approved by KBC, or for weddings, births, jubilees, retirements and religious feasts);
- gifts and entertainment offers are not accepted during a tendering procedure (up to contract signature)
- they must always be in line with good taste and decency

9 Conflicts of interest

By supplying products or services nor the supplier nor the supplier's staff acknowledges to have a conflict of interest with KBC. Supplier and supplier's staff shall avoid business activities that could or would lead to conflicts of interest between own interests and those of the KBC group. Any intervention, pressure, influence, wish or request that could jeopardize neutrality in decision-making with regard to issues involving customers or business partners is to be avoided.

10 Representation and authorization

In business relationships, KBC is always represented by a particular member of staff. In such relationships, KBC members of staff communicate directly with stakeholders and participate in building long-term business relationships. Consequently, all signature and decision-making requirements and trading limits must be observed and the necessary authorisation must be obtained. KBC may only be entered into commitments to the extent that the requisite authorisation has been granted.

11 Equal treatment/prohibition of discrimination

KBC does not tolerate discrimination or unequal treatment of its staff or customers, regardless of whether it is direct or indirect or based on race, sex, marital status, sexual orientation, age, family status, disability, religion etc…

12 Narcotics

All acts linked with narcotics or addictive substances during working hours could lead to KBC suffering a significant loss of reputation or financial damage. Supplier's staff members shall not work under the influence of drugs or alcohol.

13 Dress code

A professional attitude is a pillar of customer trust and satisfaction. Supplier's staff working on KBC premises shall be dressed neatly, in accordance with the general standards on smart business clothing.

Supplier's staff who have direct contact with KBC customers endorse a neutral stance with regard to the expression of their political, philosophical or religious beliefs in the workplace

14 Protection of KBC property – conduct for use of means of communication

KBC provides multiple means of communication to supplier's staff to operate efficiently (like PCs, telephones, internet and data access, etc.). These means of communication must be used within the professional context for which they are intended and in compliance with the rules of conduct for the use of means of communication as described in the next chapter.

Scope

KBC Group expects you use these means in a respectful and sound manner, based on the KBC company values and on the expected high level of responsible behaviour. In some businesses or in specialised activities (e.g., in the dealing rooms), the use of means of communications can be harshened with more specific rules of conduct.

This chapter applies to all means of communication provided by KBC and defined in a broad sense. They include:

- Physical means: a desktop, a laptop, a tablet, a phone, a cell phone, a smartphone, a printer, a scanner, a USB-stick, dongles, a webcam, etc.;
- Virtual means: software in general, informational applications, transactional applications, communication and collaboration tools, internet browsers, wired and wireless network connections, etc.;
- Keys: authorisations, passwords, access rights, etc.;
- Data: all kinds of confidential and non-confidential information (e.g., trade secrets, copyrights and trademarks, information regarding strategy, products or services, business plans, concepts, research and development, source codes, customer data, prospect data, supplier data, employee data, processes, business policies, practices or methodologies, etc.);
- Security: exposure to malware, viruses, hacking, cybercrime, data leakage, etc.

General prohibitions on use of means of communication

- use offensive language or transfer data/messages with offensive content or in case of undesired intimacies
- participate in/promote illegal activities;
- access, download, save, transmit or display sexually explicit, racist, insulting, intimidating or unlawful material or content;
- act in a manner that is opposed to common decency;
- use KBC's means of communications to perform personal or commercial business (without a connection to the KBC) tasks;
- nose around in/view company data and applications which are not related to your job;
- use KBC's means of communication to gamble or visit lottery websites;
- hacking computer systems or networks; unsolicited commercial advertisements ("spam");
- impersonating others.
- Jeopardizing KBC's computer systems – Introducing viruses, Trojan horses or other software which my jeopardize the confidentiality, availability and integrity of the data.
- Use against KBC's interests – dissemination of chain letters (even for charitable purposes); participation in games; personal matters with a view to profit (selling, advertising, etc.); dispatching trading advertisements in connection with (but without approval of) KBC group.

Data protection & confidentiality

You are personally responsible for all information you obtain to carry out

your tasks. Any such information may only be used to the extent necessary to carry out your tasks. Use for other purposes is prohibited. Accordingly, you must treat as confidential:

- all personal information and data regarding the assets and financial situation of customers (both natural and legal persons);
- general business information about the activities, results, employees, accounting and strategy of the KBC group;
- any data for which the confidentiality is unclear.

Never send confidential data to unauthorised persons (in or outside KBC) and take necessary protection measures when dealing with confidential information

Security

General – You can only request authorisations and access to data that are necessary for your job. If you no longer need something, take the necessary steps to cancel your access. You may not store any KBC business information or customer information on non-KBC equipment (e.g., a personal PC). In the event of any incident or abnormality (e.g., a virus) which may impact security, immediately contact the KBC Help Desk or Service Centre.

You're not allowed to change any default security-related settings (e.g., browser or email security settings) or disable security software. Security measures must remain operational at all times.

Passwords – Your access to the KBC systems, networks and data is personal and non-transferable. All passwords assigned to you must remain confidential and personal, as they are your signature attesting the use of authorizations and information granted to you. You are liable for everything that occurs under your user ID and password. Never use anyone else's user ID or password. Never share passwords/certificates/dongles to circumvent license agreements.

Protect your passwords and do not communicate them to anyone, do not write them down, or store them in legible text. Never use any of your KBC user IDs or passwords externally (e.g., for external website accounts). Choose your passwords carefully — e.g., do not choose the name of a family member, or personal date that is obvious or easy to guess. Change your passwords immediately in case of (possible) discovery.

Shared user IDs and passwords are not allowed.

Malware – Be cautious towards files received from external sources. Viruses and malware are not only contained in executable files, but also in seemingly innocuous data files (e.g. MS Word or Excel files).

Breaching security – You may not search the IT systems for "interesting" files. You also may not read or observe data of KBC's employees, customers or third parties which are transported via KBC systems. You may not (attempt to) use any software or hardware capable of evaluating or breaching system security on KBC systems or networks.

Calendar and email

If you are provide with a KBC email address, you will also have access to an electronic agenda.

- Never send confidential information to unauthorized persons. Use additional layers of protection for emails and documents with confidential information (e.g., encryption, link to documents on a secured drive, 'zip' files, etc.).
- The synchronisation of your personal and work calendar is, in principle, not allowed, except if this can be done in a controlled environment (subject to approval by Information Risk Management). If applicable, KBC will set up specific guidelines for this.

You may not:

- access or attempt to access emails which are not addressed to you;
- modify headers or attempt to falsify the content of an email and/or the ID of a sender or an addressee;
- sending out non-business related emails/messages (e.g., chain emails) or emails/messages with insulting, offensive or unethical content.
- Send or receive messages to your personal email address without KBC's prior approval. The same applies to bulk forwarding of messages in your mailbox to outside email addresses. To preserve the availability of the KBC network, transmitting and receiving voluminous files via email is automatically limited.

Use of internal communication systems and devices

- Mind your communication language and etiquette and consider the content of your message. Make sure that you don't disturb your colleagues of KBC staff when you attend a virtual meeting or a telephone conference. If possible, try to attend in a meeting room or a cockpit and choose the phone's "meeting" option when you are in a meeting..
- Be aware of your surroundings when you use your telephone, regardless of whether or not it is a company owned device. Confidential information can easily be eavesdropped on.
- Introduce yourself when you enter a teleconference or a virtual meeting and make sure that you log out of the meeting tool correctly when you leave the meeting.
- Do not share authorisations and/or call-in codes for virtual meetings or telephone conferences or make them available to unauthorised users, by putting these codes on internal drives or in calendar entries without protecting them

The use of mobile phones may be forbidden in certain locations (e.g., the trading and dealing room) or for certain activities

Internet sites and platforms

Accessing Internet websites or platforms is not a "right". You can only obtain access if warranted to execute your obligations towards KBC. Note that some categories of websites will always be blocked and that a request for access to such a site will always be rejected (e.g., in case of blocking due to unethical nature or security risks). Online submission of credit card numbers belonging to KBC is only allowed with the express agreement of KBC. Do not place any references to KBC websites, e-mail addresses or mailboxes on websites without explicit authorization from KBC.

Hardware and software

KBC provides you with all kinds of hardware, software and internal applications as a job aid. We expect you to use these prudently and that you return them in good condition when you complete your job or assignment.

Hardware

You may not disconnect any equipment from the KBC network and reconnect it to the KBC network again elsewhere. You may only connect portable PCs to the KBC network within KBC company buildings via the connections provided for this purpose and at the agreed locations. You may not connect any hardware from outside the company to the KBC network. Using the Wi-Fi-connection in KBC's premises is subject to additional terms, to be accepted before the connection is used.

You may not change anything in the configuration of the PC that is provided by KBC. Only staff of the Help Desk or the Service Centre may carry out such tasks.

Software

You may only use software for which authorization is granted. You may not bring any software with you or download and install it yourself, even if you or your company has an active license. Do not unlawfully copy any copyright-protected material (not even for your own use) and make no copies of software installed on KBC hardware. KBC reserves the right, at any time and without prior warning, to check and if necessary delete any software installed on KBC hardware.

- Make sure that your desktop, laptop or own device gets all software updates provided by KBC.
- Never remove or disable the security software of your devices.

Lock your PC whenever you leave it behind (e.g., for a break), and always store portable computers securely when you are not using them. They must never be left unattended in a car or in public transport.