How we deal with information, communication and company resources

Sub-code 3

How we deal with information, communication and company resources

We safeguard corporate information and personal data

We are conscious in our communication and our use of company resources

Contents:

The KPN Code of Conduct is applicable to all KPN employees, including the Board of Management, the Supervisory Board and temporary staff. Supplementary rules apply to certain specific functions and positions. These rules are set out in separate codes, entitled 'Insider Trading', 'Retail', 'Customer Service' and 'Engineers'. The staff concerned will be given further information by their line managers.

1. Corporate information

1.1 Complete and reliable information

We offer full transparency about our activities, performance and (financial) situation. We provide honest, accurate and readily comprehensible information. Everyone within the organization is responsible for ensuring that KPN's administrative records are up-to-date, reliable and accurate, so that we can provide internal and external stakeholders with the information they require. The records must include:

- Activities and the related transactions;
- Assets, liabilities, revenue and costs;
- All accounting entries in the correct accounting period and the correct ledgers;
- All documents which support internal and external reports.

1.2 Classify information carefully

KPN has certain information which must be restricted to authorized persons only. To simplify procedures for protecting this information, we apply four levels of classification:

- ***Unclassified (public):*** information which may be freely distributed within and beyond KPN, such as folders, product descriptions and the published Annual Reports.
- ***For internal use only:*** information which is restricted to KPN employees, such as work orders, service tickets or technical documentation.
- ***Confidential:*** information which is restricted to authorized persons on a 'need to know' basis, such as personnel records, customer data and department plans.
- ***Secret:*** information which is restricted to a very small group of (senior) staff, such as financial statements which have yet to be published.

Information is classified so that all users know how to use it and to whom it may be distributed.

For detailed instructions, see the Classification Rules section of the KPN Security Policy (KSP-FA03GL01). If you have any questions, contact Security.

1.3 Secure commercial information

You must ensure that unauthorized persons are unable to access any classified information. To do so, restrict the number of recipients and observe all security rules of the KPN Security Policy (KSP) when preparing, sending, processing or archiving classified information. Never send commercial or business information using a personal social media account. KPN has several corporate social media accounts through which we publish information intended for the general public.

All corporate and commercial information remains the exclusive property of KPN. If you leave the organization you may not use this information on behalf of your new employer. Similarly, KPN does not wish to be given information from or related to your former employer, particularly where it could impede fair and open competition.

1.4 Process and send corporate information securely

Never store or send commercial information using public (Cloud) services such as Dropbox, iCloud, Google, WeTransfer, WhatsApp etc. If we wish to share large files, we use our proprietary software. Information to be shared with third parties must always be encrypted. Secure the files with a password and send the access codes through a different channel, such as an SMS (Short

Message Service or text message). Confidential corporate information must never be placed on the internet or on TEAMKPN Online. This restriction also applies to audio-visual materials showing KPN personnel, building, sites, technical areas or the security arrangements for any system or location.

Business email must always be sent and received through an official business email account.

1.5 Protect commercial information against unauthorized access

When leaving yur desk or office, we ensure that unauthorized users cannot access commercial information. We lock our computer (Windows key + L). Information which is classified as 'confidential' or 'secret', whether on paper or in digital form, must be kept under lock and key at all times, even when working at home. Never leave corporate information unattended in public places or in your car.

Detailed instructions can be found in the KPN Security Policy (KSP) on TEAMKPN Online, under Security.

1.6 Destroy information which is no longer required

We do not store information for longer than necessary. There are set minimum and maximum retention periods, which vary according to the nature of the information, its purpose and security classification.
To dispose of documents, use a paper shredder or place them in the secure container for confidential documents. Documents with a 'secret' classification must never be placed in the container for confidential documents: always use the paper shredder. Where confidential or secret information is stored on digital media such as USB stick or external hard disk, the media must be handed in to the nearest IT Service Point (see TEAMKPN Online) at the end of the retention period. The hardware will then be 'wiped' using a certified secure process and/or physically destroyed.

1.7 Refer all press enquiries to the Media Relations department

Only members of the Board of Management and the Media Relations team may make statements to the press or answer press questions. Refer all requests and enquiries to Media Relations: (070) 44 66 300 or press@kpn.com.

When giving a presentation or speaking at a conference, remember that any information you reveal can be published (e.g., through social media). It can become global knowledge within minutes. You should always consult your line manager and KPN Media Relations beforehand to determine what may and may not be included in your talk.

1.8 Social Media

Your profile on social media may show that you work for KPN. If you state personal opinions or take part in a public discussion, be aware that other users could link your views to KPN. If any comments or complaints about KPN come to your attention, contact the webcare team at webcare@kpn.com. Our specially trained webcare agents will then respond on behalf of KPN.

2. Customer data and privacy

At KPN, we regard and handle all customer data as private and confidential.

Improper use of personal data is a violation of the customer's privacy. The manner in which to process data is therefore subject to strict conditions. We apply the 'Golden Rules for Privacy' to all customer data which we collect or keep, regardless of whether we look at the information. The Golden Rules apply when we analyse or send customer data, use it for marketing purposes, make it available to third parties, and even when we are anonymizing data or destroying it altogether.

Customer data remains sensitive until it is completely and irreversibly anonymized. That means that there must be absolutely no way in which it is possible to identify the person or persons concerned. This can be difficult to achieve and the conditions are therefore very strict. Before processing any anonymized information, contact the Privacy Office at privacy@kpn.com.

The Golden Rules for Privacy

1. We process personal data only for predefined approved purposes.

We may use personal data for the following purposes:

- executing the contract with the customer
- technical provision of services
- billing
- system administration (including network management, fraud prevention), compliance with law and regulations, market analysis and direct marketing (personalized offers).

All these purposes can be justified but the use of personal data is only permitted if the Golden Rules for Privacy are observed in full.

2. We process only as much personal data as is necessary for the intended purpose and only for as long as necessary.

We keep only the personal data that is strictly necessary to allow us to do our work effectively. We always aim to minimize the quantity of information obtained and the period for which it is retained. We always apply privacy-by-design.

Customer information must only be shared with colleagues who need it to perform the contractually agreed activities. Ask for details of those activities before sharing information.

The maximum retention period should never be exceeded. That period varies according to the type of information and the purpose for which it was obtained.

3. We process personal data only when the customer has been informed of our intention to do so.

We inform customers that their personal data may be used for certain purposes by means of privacy statements, the general terms and conditions and the product application forms. All the processing of personal data is registered. The registration is managed by the Privacy Office. We register with whom we share the data, how we keep the information and the reason why we use the personal data. When asked for, we need to give access to registration to the Dutch Data Protection Authority (DPA).

4. We use personal information for commercial purposes only with the customer's explicit consent.

The customer's consent is required before any **contact information** (name,

address, email address) or **usage information** (call minutes, number of text messages, data transfer volume) are used for market analysis or direct marketing purposes. Customers are informed about such usage and are given the opportunity to 'opt out'.

Traffic information (such as numbers called, time duration of telephone calls, web sites visited, television programmes watched, ordered or recorded) may only be used for market analysis and direct marketing if the customer has been informed in advance and has given explicit consent. The customer must 'opt in'.

Consent cannot be obtained by means of a privacy statement or the general terms and conditions. The customer must give *informed* consent, which means that we must clearly explain what information we wish to use and why. The customer must actively grant permission (e.g. by ticking the box marked 'yes'). The customer can withdraw consent at any time.

Always respect the customer's choice. If the customer has objected to the use of his or her personal information (opt-out) , or has not given the required consent (opt-in), you must not use the information.

There are certain types of personal information, known as **'profiling data'**, which KPN will never use for any purpose. They include details of religion, ethnicity, political affiliation, union membership, health status, sexual orientation and the customer's Social Security Number ("Burger Service Nummer" or "BSN").

5. We record, use or divulge the content of customers' communications only in very limited circumstances.

The confidentiality of communications (such as telephone calls, emails and text messages) is protected by law. It is a criminal offence to intercept or otherwise access the content of any communication of which you are not the intended recipient. At KPN, we never read the content of any communication. We process content only insofar as is strictly necessary to fulfil technical requirements, to maintain the integrity and security of our networks and services, to comply with a legislative directive or judicial order, or with the explicit consent of the customer concerned.

6. If providing personal information to third parties, we ensure that all privacy rules are observed.

KPN does not sell personal information to third parties.

If access to personal data is granted to any third party acting on behalf of KPN, we will enter into a formal contract with that third party, known as the 'processor'. If the processor is located outside the European Economic Area, the agreement will be in the form of the 'EU model clauses for the transfer of personal data to third countries'.

If in any doubt, contact the Privacy Office at privacy@kpn.com.

3. Company resources

Taking care of the resources provided by KPN

All resources issued to you by KPN are for your personal use only. They remain the property of KPN at all times. This also applies to access cards, user name-password combinations, etc.

- Company resources are intended for business use only. Limited private use is however permitted. KPN reserves the right to inspect or examine company resources if there is any reason to suspect misuse.
- Every effort should be made to safeguard company resources against misuse, loss, theft or damage. They must never be left unattended. Any loss or (suspected) theft should be reported to the KPN Security, Compliance and Integrity Helpdesk on 0800 – 40 40 442, email securityhelpdesk@kpn.com. You can be held personally liable for any loss caused by your own negligence.

We always handle digital resources with respect and:

- Do not open or view any web site with illegal, offensive or degrading content.
- Do not share or display any material (text, images, videos, etc.) which others may find offensive.
- Communication should be conducted in a cordial, respectful manner. Avoid controversial or potentially offensive topics.
- Do not respond to unsolicited mail but send it as an attachment to the KPN Security, Compliance & Integrity Helpdesk via securityhelpdesk@kpn.com. Be suspicious of any email you are not expecting and from a sender you do not know. Do not open attachments

unless there is a good reason to do so, having first saved the file to your hard disk (where it will automatically be scanned for viruses).

- We are all responsible for maintaining the integrity of the KPN network. Do not send or download:
  - Software which may compromise the systems (viruses, malware, spam, etc.)
  - Large (executable) files unless using our own software and/or they are encrypted
  - Emails to large groups of recipients (mailing lists) unless with the approval and assistance of Corporate Communications.
- Do not alter the configuration or settings of any software installed on the workstation computers. Software may not be installed on a computer unless expressly approved by KPN.

4. Insider information

Insider information refers to the possession of information about KPN which is not yet in the public domain, the publication of which can affect the stock market value of the company.

By law, it is illegal to trade in shares or derivatives if you possess such information. It is also an offence to pass this knowledge on to someone else.

Specific rules apply to staff who, by virtue of their function, have regular access to insider knowledge. These rules are set out in the part-code ‘Subcode Insider Information ’. Further information will be provided to the staff concerned.

5. Information, advice and reporting

We speak-up about compliance with the KPN Code of Conduct and sub-codes, regardless of position or function within the organization. You must familiarize yourself with the content of the relevant codes, and comply with it at all times. Line managers oversee compliance and create an atmosphere in which matters can be discussed openly. If you disagree with a colleague and are unable to resolve it, contact your line manager, HR consultant or the confidential advisor (staff counsellor).

If you have any questions about a code or are experiencing an (ethical) dilemma you do not wish to discuss with your line manager, contact the KPN Security, Compliance and Integrity Helpdesk. You can also report any irregularities anonymously via the SpeakUp Line.

The KPN Code of Conduct and sub-codes present rules of conduct. These rules are binding and compliance is mandatory. Based on reports of (suspected) misconduct, the activities and behavior of employees can be investigated taking due account of the applicable procedures. Any violation can lead to disciplinary action as provided by the KPN Collective Labour Agreement (CAO). Depending on the circumstances, sanctions range from a written warning to instant dismissal.

Information, advice and reporting

1. Contact your immediate line manager
2. Contact the KPN Security, Compliance & Integrity Helpdesk 0800 - 40 40 442 or securityhelpdesk@kpn.com
3. Contact the confidential advisor: see KPN Vertrouwenspersoon
4. Anonymously, via the KPN SpeakUp Line:
   0800 - 02 22 931 (login code 57660)