Fraud policy

Measures against white collar crime and serious misconduct.

Decided by the Board of Management on February 7, 2006

Deutsche Telekom

Table of contents

1 Preamble

According to current studies, companies are increasingly becoming victims of white collar crime. The offenders are in many cases from the company's own ranks.

White collar crimes lead to year-on-year losses running into billions for the companies concerned and for the entire economy. Often these damages are accompanied by intangible consequential damages, such as damaged reputation with investors and the general public, reduced motivation among employees and a detrimental effect on relationships with business partners.

The effective defense against such threats and the consistent action against white collar crime therefore forms part of permanent challenges and are important components of a responsible corporate policy.

In the Deutsche Telekom Group too, white collar crimes and other deliberate misconduct are not acceptable and must be punished in a consistent manner.

Against this background, the Board of Management at Deutsche Telekom decided on May 9, 2005 to protect the tangible and intangible assets of the company and to set up a Group-wide standardized anti-fraud management in the interests of all its shareholders.

The objective of anti-fraud management is to create Group-wide structures which should ensure that white collar crimes and other serious breaches of important compliance requirements are prevented, detected and pursued.

Anti-fraud management is an integrated component of a Group-wide compliance management and part of the corporate culture of the Deutsche Telekom Group.

This policy presents the important basic principles and elements of the Deutsche Telekom Group's anti-fraud management and contains instructions and recommended actions for handling cases of fraud in the company.

It should help the managers and employees of the Deutsche Telekom Group to take the necessary measures to prevent and combat fraud, and to support efforts in all areas to protect the company from the risks caused by fraud. Furthermore, this policy should promote discussions and the process of sensitization at all levels in the company and increase the awareness of problems concerning fraudulent behavior.

2 Scope of validity

This policy applies to all cases of fraud involving:

- bodies and employees of the Deutsche Telekom Group
- consultants, customers, suppliers and other business partners of the Deutsche Telekom Group
- representatives of private and public institutions with which the Deutsche Telekom Group has business relationships
- shareholders and investors

and by which the Deutsche Telekom Group - with its legally independent or legally dependent units - is affected or may be affected.

This also includes cases in which initially there are sufficient factual basis of the suspected occurrence of fraud.

The policy applies for Deutsche Telekom AG with its direct and indirect majority holdings.

3 Fraud definition

Fraud in terms of this policy is any deliberate or negligent breach by bodies, employees or third-parties of:

- capital market-related provisions, if and to the extent to which they relate to the Deutsche Telekom Group,
- laws, if and to the extent to which the breach of pecuniary interests has or may have consequences for the Deutsche Telekom Group

  or

- company-internal guidelines, if and to the extent to which these are determined to protect the pecuniary interests of the Deutsche Telekom Group and its individual enterprises.

In compliance with this definition, the following will be deemed to be fraud, but not exclusively:

- Breach of trust
- Deception and capital investment deception
- Theft and embezzlement
- Robbery and blackmail
- Corruption (personal gain, granting advantages, taking or giving bribes)
- Coercion and threats
- Offenses concerning manipulation of accounting and financial statements
- Insider dealing
- Manipulation of rate or market price
- Falsification of documentation and other manipulative actions to documents
- Computer offenses
- Piracy of products and brands
- Betrayal of private or business secrets
- Insolvency-related crimes
- Anti-competitive arrangements
- Money laundering
- Violation of purchasing policies
- Violation of representation and signature-authority rules
- Violation of private investment group policy

4 Basic principles

The cooperation of everyone is required for the successful defense against the risks posed by fraud. All employees should make a personal contribution to ensuring that cases of fraud can be averted, detected and pursued in order to protect the tangible and intangible assets of the Deutsche Telekom Group and its public reputation.

If employees receive private or business information which, after duty-bound personal review suggests a specific suspicion of fraud, they are obliged due to their contractual loyalty obligations to inform their employers of this. Notification may take place in particular via the channels listed in 5.4.1. If there is any doubt about the existence of sufficient factual indications of suspected fraud, the contacts to be named in accordance with 5.1will provide advice and assistance in assessing the facts.

4.1 Responsibilities

The management in all legally independent and dependent units of the Deutsche Telekom Group is responsible for all measures concerning the prevention and detection of fraud in their respective business area.

The units of the Deutsche Telekom Group must comply with all applicable, valid legal provisions in force without limitation. In the event of ambiguities and doubts about the applicability, validity and effectiveness of legal provisions, the relevant responsible internal legal departments must be consulted.

The units of the Deutsche Telekom Group must in particular observe and meet the general and special requirements with the due care of a conscientious businessman. These duties of care include the following organizational duties.

4.2 Organizational duties

The Board of Management of the Group and the management will guarantee:

- Clear organizational structures
- Clear responsibilities
- Clear delineations and limitations of internal authority
- Compliance with appropriate principles of a proper delegation of tasks and obligations.
- Careful selection, briefing (training/information) and monitoring of delegates
- Obtaining and complying with legal advice from the responsible internal legal department regarding all legally relevant situations.
- Allocation of tasks according to substantive responsibilities and skills
- Observance of the principle of cross-checking individual decisions by another company representative
- Clear representation and signature rules
- Monitoring through Auditing or external auditors
- Reporting on the cases of fraud which occur in the Deutsche Telekom Group at regular intervals and as justified.

Management and employees will observe the following basic principles when delegating tasks:

- Careful selection of delegates according to technical and personal suitability
- Avoidance of transfer of duties and responsibilities too far down the hierarchy of authority
- Prevention of excessive demands on delegates
- Instructing delegates in a unambiguous, clear and complete manner
- Regular monitoring of specialized knowledge and reliability of delegates
- Intervention in the event of misconduct by delegates through clarification of the facts, investigation and the future elimination of the sources of the problem

5 Measures

5.1 Contacts for anti-fraud management

Depending on the task and the size of the organizational unit, contacts for anti-fraud management will be named for all organizational units and made known in a suitable manner.

5.2 Risk analysis – fraud risk assessment

An important basis and condition for an effective and efficient defense against fraud is the systematic recording and analysis of fraud risks within the Deutsche Telekom Group and the fraud cases which have been discovered or otherwise become known in some way.

In order to identify organizational, HR and situational risk potential, different units (e.g. Procurement, Human Resources, International Accounting, Corporate Security, Auditing) will carry out a fraud risk assessment (FRA) (i.e. an investigation into the fraud risks existing in an area) at regular intervals and as justified and present which controls exist for the detection and prevention of fraud in the relevant area or which measures are suitable and recommended for the reduction or removal of identified fraud risks in the structure and operations of the organization.

5.3 Prevention – fraud prevention

5.3.1 Information

Employees should be made aware of the risks of fraud and advised about fraud sanctions at the time of employment and when they change jobs within the Deutsche Telekom Group. As regards possible fraud risks, employees should also be made aware of these subsequently. If involved in activities in organizational units with an increased risk of fraud, employees should be reminded of this and given more in-depth training for their specific work responsibilities at regular intervals.

The internal organizational units for education and training, as well as staff development, will include the topic of “anti-fraud management” in their programs. The need to train managers and employees in organizational units at particular risk should be taken into consideration in particular.

5.3.2 Selection and deployment of staff

The reliability and personal integrity of employees is an important factor in the reduction of fraud risks in all areas of the Deutsche Telekom Group.

The processes for filling positions should therefore be designed to enable a reliable assessment of the technical and personal suitability of the job applicant. Superiors are responsible, as part of an active and fore-sighted HR management and control, to check the continuity of the personal and technical suitability of their employees at regular intervals or with good reason.

In areas in which, according to the outcome of the fraud risk assessment carried out, the personal and technical unreliability and the duration over time of the employee’s performance of the same tasks represent the increased risk factors, when filling positions careful attention should be paid to the suitability of applicants from a technical and personal perspective. In these areas, a periodical change of function of employees should also be considered as a possible tool for reducing the risks of fraud. A change of function is the same as a change of task layout which ensures that the responsibility of the employee in their new task area spans another group of people. With a periodic change of function, the personal interests of employees, in particular as regards the timing of the change of function, should be taken into account as far as possible. If a periodic function change stands in the way of urgent practical and economic reasons (e.g. lack of suitable personnel or positions of same value), other preventative measures should be encouraged and documented.

5.3.3 Organizational control mechanisms

Business decisions must be transparent in every phase, including the preparation for decisions..

Transaction-related verbal explanations and information should always be carefully documented in writing. The documentation accompanying the transaction must give a full and precise account of the individual steps in transaction processing. Notwithstanding legal duties of retention, documentation of significant transactions must be archived in a suitable form.

In the business process, suitable measures for transaction controls must be planned (e.g. resubmissions, final comments, random checks of discretionary decisions). These measures serve to protect employees and should make it clear that there is a high probability of detection. Particularly intensive control measures are required in areas in which there is an increased risk of fraud according to the outcome of the fraud risk assessment conducted. The execution of control measures should be documented such that it can be traced.

Organizational measures, in particular regulations on responsibility, should be taken so as to minimize fraud risks. Above all, this includes regulations according to which several people have to contribute to the decisions (double-checking principle). This may occur by dividing up decision-making competences or by extending control options. Where possible the double-checking principle should be encouraged.

5.4 Clarification of facts – fraud detection

If there are specific indications of fraud, the facts will be investigated further without regard to the standing of the suspect and his or her position in the company.

In so doing, the circumstances that both incriminate and exonerate the suspect must be investigated.

5.4.1 Duties of employees and superiors

Employees who acquire knowledge of facts privately or during business which form the basis of suspected fraud are obliged due to their contractual loyalty obligations promptly to inform their employers of this. The following offices and/or persons in particular will receive the appropriate information:

- immediate superiors
- indirect superiors or
- contacts named by the organizational units.

Instead of notifying the previously named offices and/or persons, the following paths can also be used for notifications:

- EthikLine
- Business Keeper Monitoring System (BKMS).

Notifications with regard to suspected fraud must be handled with heightened confidentiality.

Once they receive specific indications of fraud, the offices informed must immediately consult the organizational units responsible for investigating facts in cases of suspected fraud.

5.4.2 Responsibilities and procedure

The investigation of facts due to suspected fraud lies exclusively in the hands of the organizational units and persons responsible according to the corporate division of responsibilities.

The individual units of the Deutsche Telekom Group are responsible for complying with the appropriate responsibility regulations for processing fraud cases and determining processes for the investigation of facts within the respective unit and when comparing units with one another.

In the interests of uniform manner of handling cases, the following principles should be considered:

Units or persons who are not responsible are not allowed to carry out their own measures for the investigation of facts without being commissioned by or without prior approval from the responsible organizational units.

The investigation of facts should be carried out efficiently and not extend beyond that which is absolutely necessary to prove the personal responsibility of a suspect. In so doing it must be ensured that later investigations by criminal authorities are not jeopardized.

With regard to the possible measures relating to employment law, public servant law, civil law and criminal law, the legal and HR departments responsible must be integrated at an early stage.

When carrying out searches exercising the right to ban somebody from the premises, an affiliate of the legal department responsible or another person must be used as a witness to the search. This does not apply where immediate action is required and provided due to a risk that evidence will otherwise be lost.

The suspect should not be questioned in relation to measures concerning employment law and civil servant law until after approval with the responsible legal or HR department.

The responsible legal and HR departments will in principle decide on the measures concerning employment law or civil servant law and civil law (work suspension for the suspect, preservation of damage claims) to be implemented immediately, and if appropriate, limited to a fixed period of time .

All steps in the investigation of facts and the outcome of the individual investigation measures must be documented in writing - both in full and carefully – in a manner which can be traced by a third party. For evidentiary and investigative purposes, the documentation on the clarification of facts should be integrated with the documentation on HR, legal and organizational follow-up measures to create a standardized process document.

In an internal investigation of facts due to a suspected offense, the responsible legal department will check whether the legal and factual requirements for reporting an offence to criminal authorities exist, based on the conclusions made and the evidence unearthed. This excludes cases which do not feature any problems from a factual and legal point of view as well as cases in which the preliminary proceedings with criminal authorities are already pending.

Subject to a case-specific review a criminal complaint should in principle be reported in cases in which the assets of the Deutsche Telekom Group have been directly damaged through fraudulent behavior.

The communication with criminal authorities in connection with preliminary proceedings should in principle be carried out by or in consultation with the responsible legal department.

5.4.3 Protection of the suspect and confidentiality

As regards the decision to initiate an investigation, anonymous information, rumors from external sources or insinuations by colleagues must be investigated and analyzed with particular care so that any misuse can be eliminated to the greatest possible extent.

When investigating facts, the personality rights of the suspect and the general constitutional principles, in particular the basic principle of reasonableness and the prohibition of excessiveness shall be observed.

The gathering of evidence must only take place using legally permissible means. If there is any doubt as to the legal validity of individual investigatory measures the responsible legal department must be consulted.

While investigating the facts, any actions which are not part of the investigatory measures which could result in the exposure of suspected persons must be avoided. This applies in particular to written correspondence between the organizational unit responsible for the clarification of facts and other organizational units and persons as well as during the questioning of witnesses. Where a personal description of a suspect or the suspicious circumstances

he/she is accused of is unavoidable, it must be made clear that only the suspicion of fraudulent behavior is in question.

Personal data must be handled according to the data protection regulations in the Deutsche Telekom Group and the relevant legal data protection provisions.

Persons and units will only be informed of any suspicious behavior or the results of determinations if they can prove they have a justified interest in such information.

5.4.4 Protection of the informant

The basic principle that any reports concerning suspected fraud must be treated with particular confidentiality also applies in particular to the informant.

The Deutsche Telekom Group shall take all necessary and reasonable measures to guarantee that persons who have provided information about fraud or corresponding cases of suspicion in good faith do not suffer any personal, business or financial disadvantages.

If messages are sent via the security-certified Business Keeper Monitoring System (BKMS) the absolute and permanent anonymity of the informant is guaranteed.

5.5 Sanctioning of fraud

The information published on the Deutsche Telekom AG intranet in the TeamNet Special for T-Spirit on handling misconduct and the sanction options gives managers and employees examples of how misconduct can be dealt with according to employment law, civil services law and criminal law.

5.6 Information about cases of fraud discovered and monitoring

The Audit Committee must be informed at regular intervals of any fraud cases which become known and the personal, legal and organizational follow-up measures taken relating to these.

Any notification of the public of the cases of fraud detected will take place only through the responsible corporate communications after prior agreement with the responsible legal department .

Informing the bodies and the internal and external public must not jeopardize internal factual investigation of facts and the investigations by the criminal prosecution authorities.

When passing on this information it must be ensured that the legitimate interests of the persons concerned are not adversely affected.

The units responsible for anti-fraud management or special bodies still to be named will check the quality of processes relating to the processing of fraud cases at regular intervals or upon request.

6 Final provisions

This policy will enter into force after employees have been notified.

The provisions in this policy will be checked once a year for any necessary modification or adaptation by Legal Affairs at Deutsche Telekom AG.