

DE NEDERLANDSCHE BANK N.V.

## **Regulation on Careful Handling of Information**

### Artikel 1

For the purposes of this Regulation the following definitions shall apply:

- a. *DNB*: De Nederlandsche Bank N.V.;
- b. *digital resources*: resources made available by DNB to the employee on which digital information can be stored, and facilities for the exchange of information via digital media;
- c. *employee*: the person who works for DNB;
- d. *information*: set of interrelated data, to which a certain significance can be attached and to which the employee is given access in the context of the performance of his duties.

### Article 2

This Regulation shall apply to all employees of DNB.

### Artikel 3

In handling information, employees shall observe the obligations of confidentiality that ensue from legislation, the collective labour agreement and the contract of employment.

### Artikel 4

In handling information, employees shall adhere to the regulations and instructions of DNB in the area of classification and security of information.

### Artikel 5

Employees shall share information with each other if such is permitted and is of significance for the performance of their tasks and activities.

### Artikel 6

Employees shall view information not addressed to them only if such information is relevant to the performance of their tasks and activities.

### Artikel 7

Employees shall not use information for any purpose other than the performance of their tasks or activities.

### Artikel 8

- a. The manner in which employees handle information may be monitored by DNB.
- b. With respect to information that is accessible via digital resources, the 'Regulation on Monitoring the Use of Digital Resources' describes which data shall be recorded, on which

grounds such recording shall take place and in which manner and to whom access shall be provided.

## **Explanatory Notes to the Regulation on Careful Handling of Information**

### **General**

DNB and its employees deal with a large amount of confidential information. DNB's Code of Conduct prescribes that employees are to handle this information carefully and that confidential information is to be handled confidentially. The present Regulation seeks to provide a more detailed elaboration of this provision in DNB's Code of Conduct.

This Regulation contains principle-based provisions, and operates on the assumption that employees have their own responsibility in handling information. The objective of the Regulation is to create a frame of reference within which the employee must make his/her own judgment. In case of doubt, the employee should consult his/her senior officer.

The frame of reference created by the Regulation applies to all employees of DNB. The Regulation therefore takes precedence over rules and agreements made prior to the entry into force of this Regulation, both bank-wide and on a divisional and departmental level. After this present Regulation has come into force, divisions and departments that have adopted their own rules should therefore reconsider these rules.

### **Explanatory Notes to the Individual Articles**

#### Article 1

##### *Information*

The term 'information' has been broadly defined in this Regulation. An important element is that information does not only refer to data recorded on paper or on an information carrier (computer, memory stick). Verbal information (such as might be received from a colleague from another department during a social gathering within DNB) and information in a person's memory also fall within the definition of 'information' and therefore within the scope of this Regulation.

##### *Employee*

Employees within the meaning of this Regulation are understood to be any and all persons who perform activities for DNB, irrespective of the manner of their relationship with DNB. The definition of employee covers, in any case, employees on permanent or temporary contract, insourced employees, temporary workers, trainees and secondees. The only condition is the existence of some relationship of authority between DNB and the employee. It thus concerns staff members and similar employees. Therefore, independent external consultants, but also service providers such as window cleaners do not fall within the scope of this Regulation.

#### Article 3

DNB performs tasks that are based on various laws. A common feature of these laws is that they bind DNB and its employees to confidentiality. Statutory obligations of confidentiality ensue from supervisory legislation, the Bank Act, the Articles of Association of DNB and the Statute of the ESCB and of the ECB. In addition, DNB performs activities which - also without being prescribed by law - are of a confidential nature.

In compliance with the applicable obligations of confidentiality, employees are to sign a statement of confidentiality when entering DNB's employment, which statement forms part of their contract of employment. The duty of employees to observe confidentiality is not tied to a specific type of information; both supervisory information, information derived from the ESCB and other confidential information fall under this duty of confidentiality. The degree of confidentiality of the information and the corresponding obligations of confidentiality are also of influence on the manner in which employees may view and share information among each other.

#### Article 4

Information at DNB has been classified. Classification means that information is assigned to an information category which reflects the degree of its confidentiality. The information category indicates with whom the information may be shared (internally and externally).

Furthermore, DNB has in place regulations and instructions to safeguard information security. These govern the storage, transmission and destruction of information. The employee should abide by such internal regulations and instructions. An example of such an instruction is the brochure "Information security and Internet safety – Guidelines for the use of the Internet, e-mail and other digital resources".

If certain information has not been classified by its degree of confidentiality, it may not be readily assumed that the information is not confidential. In the absence of any apparent classification, the employee must form his/her own judgment about the likely degree of confidentiality and act upon it. In case of doubt, further inquiries must be made.

#### Articles 5, 6 and 7

Articles 5 and 6 stipulate that information may be shared and viewed if such is permitted *and* if it is of significance for the employee's performance of tasks and activities. Article 7 adds the provision that information may be used only for its intended purposes. If there are any doubts about the interpretation of these conditions, the employee must discuss it with his/her senior officer. Below, some explanation will be given of the terms 'permitted' and 'of significance', as well as a few examples – not meant to be exhaustive – of how to interpret these terms.

##### *'Permitted'*

On the basis of the information category assigned to it, employees can determine with whom certain information may be shared. For instance, documents classified as 'secret' are only intended for the eyes of the addressees. The recipient of such a document may not share the information in it with others, even if the information could, for instance, come in 'handy' for his/her immediate colleagues. Hence, in such a case, the sharing of information is not permitted.

##### *'Of significance'*

Information which has been classified as 'confidential' may, in principle, be shared and viewed by a wider circle of employees. This is, however, on the condition that the information is in any way significant for the recipient in his/her performance of tasks or activities. Hence, sharing information with colleagues merely because it is 'nice' to know something, does not fall into the category of being of significance for the performance of one's tasks and activities. Neither does the viewing of information in which the employee has a private interest or is personally interested. These examples fall within the category 'nice to know', whereas 'of significance' refers to what has been termed as the 'need to know'.

### *Chinese walls*

The rules about sharing and viewing information also apply when, on the basis of information categories or Chinese Walls, employees have access or can gain access to specific information. The term ‘Chinese walls’ refers to the procedures and measures that determine who has access to specific information. By virtue of their position, some employees have access to a large number of files and documents. The intention, of course, is that they can do a better job when they have access to all the information they need. It is explicitly not the intention that employees may view all the information that is accessible to them ‘for no reason’.

The conditions referred to in Articles 5 and 6 are principle-based and do therefore not indicate an exact code of behaviour for all possible instances. It is the employee’s own responsibility – with due observance of the conditions stated in this Regulation – to differentiate between what is permitted and what is not, which information is of significance and which is not. In case of doubt, the employee should consult their Senior Officer or the Compliance Officer.