DE NEDERLANDSCHE BANK N.V.

Regulation on Monitoring the Use of Digital Corporate Resources

Article 1 Definitions

a. *Administrator*: the Employee in charge of managing a system or corporate resource;
b. *Breach of Integrity*: an infringement or concrete suspected infringement of internal or external rules and regulations, where the reliability of an Employee may be in question, as referred to in the Regulation on Special Investigations into Breaches of Integrity (*Regeling bijzondere onderzoeken naar integriteitsschending*);
c. *Content Filtering*: the automated scanning and filtering of the content of e-mails and the use of the Internet by Employees;
d. *Digital Corporate Resources*: resources made available by DNB to Employees for storing or exchanging digital information;
e. *DNB*: De Nederlandsche Bank N.V.;
f. *Employee*: a person who works for DNB;
g. *Log Data*: data on the use of Digital Corporate Resources collected by means of Logging;
h. *Logging*: automated recording of data on the use of Digital Corporate Resources;
i. *Monitoring*: supervision by a manager of the use of Digital Corporate Resources on the basis of Reports;
j. *Personal Data*: any information relating to an identified or identifiable natural person;
k. *Regulation*: this Regulation on Monitoring the Use of Digital Corporate Resources;
l. *Report*: an anonymised report prepared for each section/department/division on the basis of Log Data and Content Filtering;
m. *Traffic Data*: data on the use of Digital Corporate Resources by Employees that do not relate to the content of messages or files;
n. *Wbp:* the Dutch Personal Data Protection Act (*Wet bescherming persoonsgegevens*).

Article 2 Scope

1. The Regulation applies exclusively to monitoring the use of Digital Corporate Resources.
2. In the event of a suspected Breach of Integrity, the Regulation on Special Investigations into Breaches of Integrity takes effect.

Article 3 Monitoring

1. Monitoring in the context of the Regulation is performed on the basis of a Report.
2. Reports contain Traffic Data only.
3. In principle, Reports cannot be traced back to individual Employees.

Article 4 Purposes of monitoring the use of Digital Corporate Resources

1. The use of Digital Corporate Resources is monitored only for one or more of the following purposes:
   a. monitoring of compliance with DNB's internal regulations;
   b. prevention of Breaches of Integrity;
   c. protection of DNB's systems and networks;
   d. protection of DNB's confidential information;
   e. protection of DNB's reputation;
   f. provision of management information in the context of cost and capacity control.
2. The principles of proportionality and subsidiarity are observed in any and all Monitoring.

Article 5 Logging

1. The use of Digital Corporate Resources is logged.
2. Log Data are accessible only to authorised Administrators.

Article 6 Reports

1. Using Log Data and Content Filtering, the Administrator can generate regular or occasional aggregate level Reports relating to a specific corporate resource. Aggregate Reports contain

totalised and anonymised data. Aggregate Reports are provided to section heads, department heads and division directors.
2. Any section head, department head or division director suspecting, on the basis of an aggregate Report, that someone's use of a Digital Corporate Resource violates the Regulation can ask the Administrator to prepare individual Employee reports. Managers intending to request an individual report from the Administrator require their immediate superior's permission. If an individual report is provided, the Employee in question is subsequently notified of that fact as soon as possible.
3. Individual reports contain Traffic Data that are directly traceable to individual Employees.

Article 7 Personal Data Protection Act
Within the framework of this Regulation, Personal Data are processed in accordance with the relevant requirements of the *Wbp* (and other applicable legislation).

Article 8 Retention period
1. The results of Logging and Content Filtering are retained for a maximum period of six months.
2. Data are converted into Reports as soon as practicable.
3. Personal Data processed in the context of Monitoring are not retained longer than is necessary for that purpose. DNB observes a maximum retention period of six months.

Article 9 Confidentiality
Employees must maintain the confidentiality of Personal Data of which they become aware in the context of this Regulation, except where any statutory provision requires them to disclose such data or the necessity of disclosure follows from their duties.

Article 10 Rights of Employees
1. Employees may request the Compliance Officer to inspect or receive information on a record of their Personal Data that has been made in the context of this Regulation. Requests will be answered within four weeks.
2. Employees may request the Compliance Officer to correct, add to or remove their Personal Data if these are factually incorrect, partially incomplete or irrelevant to the matter in hand, or processed in violation of a statutory provision. Requests will be answered within four weeks.
3. In special personal circumstances, Employees may object to the processing of their Personal Data in writing with the Compliance Officer. The Governing Board decides whether an objection is justified within four weeks after receiving the related notice. If the objection is justified, the Administrator discontinues the relevant processing of Personal Data with immediate effect.

Article 11 Employees with a special status
Extra care is taken in monitoring the use of Digital Corporate Resources by members of the Works Council, the company doctor and other employees in a position of trust as designated by the Governing Board.

Article 12 Complaints
1. Employees who believe that DNB has acted in breach of this Regulation or who otherwise have a complaint related to this Regulation can contact their immediate superior.
2. If a complaint cannot be resolved in consultation with the immediate superior, it may be submitted to the Complaints Committee as defined in the General Internal Complaints Procedure (*Algemene interne klachtenprocedure*).

Explanatory notes to the Regulation

Introduction
DNB wishes to have insight into how Employees use Digital or other Corporate Resources made available to them. One of the methods to gain such insight is to make an automatic record of specific use data, also called logging, and to monitor these data. This Regulation sets out how DNB monitors the use of Digital Corporate Resources by its Employees and establishes the parameters within which DNB may operate.

As Monitoring touches upon the privacy of Employees, this Regulation seeks to strike a balance between DNB's interests in monitoring the use of Digital Corporate Resources and Employees' interests in protecting their privacy. In monitoring Employees, DNB acts in accordance with the relevant requirements of the *Wbp* (and other applicable legislation).

Explanatory notes to the individual articles

Article 1 Definitions

Employees
"Employees" within the meaning of this Regulation are understood to be any and all persons who perform activities for DNB, irrespective of the nature of their relationship with DNB. In any event, the definition covers employees on a permanent or temporary contract, insourced staff, temporary agency workers, trainees and persons performing work for DNB on the basis of a secondment contract. The only condition is the existence of some relationship of authority between DNB and the Employee. In other words, it covers employees and persons considered equivalent to employees.

Corporate resources
In a general sense, the term "corporate resources" is understood to mean "resources and facilities of DNB that are used by Employees in the performance of their duties, as well as other property available at DNB", as referred to in the Regulation on the Use of Corporate Resources (*Regeling gebruik bedrijfsmiddelen*). The term "corporate resources" covers computers, but also tables, chairs and paper.

This Regulation solely governs monitoring of the use of Digital Corporate Resources. Digital Corporate Resources are defined as "resources made available to Employees by DNB on which digital information can be stored and that are suitable for the exchange of information via digital media". The term currently covers, in any case, the Internet in the workplace, e-mail, telephone in the workplace, digital filing systems, browsers, mobile phones, BlackBerries and network directories.

Monitoring may also extend to the use of Digital Corporate Resources for the purpose of storing or processing confidential information in a cloud not made available by DNB. The list in the preceding paragraph is not exhaustive. The definition of Digital Corporate Resources within the meaning of this Regulation does not cover DNB's time registration system (TRS) or access registration. All DNB Employees are familiar with the internal regulations and further instructions on exercising due care in using the corporate resources made available to them and handling confidential information. These rules also extend to the storing and processing of confidential information in a cloud not made available by DNB.

The list in the preceding paragraph is not exhaustive. The definition of Digital Corporate Resources within the meaning of this Regulation does not cover DNB's time registration system (TRS) or access registration.

All DNB Employees are familiar with the rules for proper handling of confidential information.

Personal data
The definition of Personal Data is in keeping with the corresponding definition of that term in Section 1 of the *Wbp*. In practice, this means that any and all data that can provide information on an identified or identifiable natural person are Personal Data. This also includes data that are indirectly identifying, for instance data that have been anonymised but, combined with other data, may be traced back to a particular person.

Traffic Data
Traffic Data show what Digital Corporate Resources are used when and for how long. In terms of e-mail and Internet communications, the content of messages exchanged and websites visited is automatically scanned for certain keywords by means of Content Filtering. The Content Filtering programme automatically registers the occurrence of certain keywords in e-mail messages and provides this information as Traffic Data in a Report.

Article 3 Monitoring
Monitoring is performed on the basis of Reports. In principle, Report details cannot be traced back to individual persons. The purposes of Monitoring are specified in detail in the Regulation.

It is emphasised that this Regulation aims in particular to enable managers to discuss and explain potential violations in the use of Digital Corporate Resources with their section/department/division at an early stage. Doing so allows Employees concerned to cease the use in violation of this Regulation.

Content Filtering is used specifically with a view to preventing business secrets/confidential information from being leaked (unintentionally). In practice, this means that DNB has selected search terms indicating that information potentially identified as a business secret/confidential information is leaving the organisation. Content Filtering generates a warning only for messages sent to non-DNB addresses and containing a keyword that potentially points to the presence of confidential information/a business secret.

On the one hand the introduction of Content Filtering serves to satisfy DNB's interest in preventing business secrets/confidential information (including supervisory information) from being leaked. On the other hand, its use as a monitoring tool invades Employees' privacy only to a limited extent. The intended purpose cannot be achieved by using a "lighter" instrument; it can even be argued that Content Filtering is less invasive than other monitoring methods, for instance full or random content monitoring.

Article 4 Purposes of monitoring the use of Digital Corporate Resources
The *Wbp* stipulates that Personal Data may be obtained only for specific, explicitly defined and legitimate purposes. Personal Data that have been collected within the framework of this Regulation may be processed only for one or more of the purposes specified in Article 4.

Furthermore, the *Wbp* requires that a proportionality and subsidiarity check be made. The explanatory notes to Article 3 of the Regulation contain an important comment in this respect. It emphasises the initial action to be taken by a manager, i.e. notifying the section/department/division that Digital Corporate Resources are potentially being used contrary to the purposes set out in this Regulation. It also emphasises that DNB resorts to monitoring the use of Digital Corporate Resources by means of Reports only if other measures have proved insufficiently effective to achieve the purposes set out in Article 4 (subsidiarity requirement). In addition, the Monitoring method must be appropriate for the purpose to be achieved, and it must not be possible to achieve that purpose otherwise (proportionality requirement). It is important that these requirements are always checked before it is decided to monitor the use of corporate resources in a specific manner.

The phrase "DNB's internal regulations" in Article 4.1a refers mainly to the Regulation on the Use of Corporate Resources (*Regeling gebruik bedrijfsmiddelen*) and the Regulation on Careful Handling of Information (*Regeling zorgvuldig omgaan met informatie*).

Article 5 Logging
The use of Digital Corporate Resources is recorded in a log. A user's actions with a specific corporate resource are registered at individual level. Some examples:

Use of mobile communication services and mobile data traffic
Mobile phone use and mobile data traffic are logged.

Use of e-mail
The Content Filtering programme logs elements of Traffic Data, e-mail message content and attachments possibly containing confidential information, on the basis of a series of keywords.

Use of the Internet
Website visits are logged automatically. The Content Filtering programme registers the websites visited by Employees at individual level. Sites are categorised based on content.

The log files are accessible only to authorised Administrators who by the nature of their position require access to these files. Logging takes place automatically, i.e. without human intervention.

Article 6 Reports
The use of Digital Corporate Resources is logged. Reports are prepared on the basis of Log Data and Content Filtering information. Reports are issued to management on a regular basis for the purpose of Monitoring the use of Digital Corporate Resources.

Currently, monthly Reports on the use of the Internet, the details of which cannot be traced back to individual Employees, are prepared and distributed to department heads, section heads and division directors. These Reports cover only certain types of inappropriate websites (e.g. sex, gambling, etc.) visited by Employees, and therefore do not provide insight into their total Internet usage. Standard Reports are also provided on the use of mobile communication resources, specifying the duration and costs of such use in a particular time period at individual Employee level. These costs are relevant to the organisation with a view to monitoring its operating expenses.

A manager suspecting unauthorised use of a corporate resource on the basis of a Report may lift the anonymity of the Employee in question. This implies that the Report on the relevant individual Employee shows the Traffic Data only; message content is explicitly not included. The individual Report allows the manager to confront the Employee in question with the Traffic Data suggesting that Digital Corporate Resources have been used without authority.

For instance, a Report revealing a strongly deviating use of a specific Digital Corporate Resource may be reason to prepare a report at individual level. In that case, the Administrator draws up a Report at the manager's request, with the permission of the latter's immediate superior, that can be traced back to an individual Employee.

Even so, the Report may contain only Traffic Data at individual level, in accordance with Article 6.2 of this Regulation. Individual Reports differ from aggregate Reports in that they do provide information at individual level. In the context of this Regulation, the content of e-mail messages, telephone conversations and information or files exchanged via the Internet will never be reported in its entirety. This Regulation does not allow screening of the full content of messages or files.

Suspected unauthorised use of Digital Corporate Resources need not necessarily involve a Breach of Integrity within the meaning of the Regulation on Special Investigations into Breaches of Integrity. If, for instance, Monitoring brings to light excessive private use of corporate resources, or any other breach of DNB regulations, the manager may speak to the relevant Employee about it. This may be

enough to settle the matter. If Monitoring gives rise to a concrete suspected Breach of Integrity, this may be reason to make a report, which in turn may warrant a special investigation within the framework of the Regulation on Special Investigations into Breaches of Integrity.

This Regulation refers to "anonymised data" and "anonymous data". It is emphasised that for these purposes the Regulation does not follow the definitions of these terms given by the Dutch Data Protection Authority (*College bescherming persoonsgegevens*). In referring to the terms "anonymised data" and "anonymous data", this Regulation stresses that, in principle, managers cannot use Reports to establish the identity of individual Employees behind Traffic Data. However, the terms "anonymised data" and "anonymous data" used in this Regulation explicitly do not mean that it is technically impossible to link a certain set of Traffic Data to an individual Employee.

Article 6.2 stipulates that requests to the Administrator for individual reports are granted only if the manager making the request has the immediate superior's permission. Reports relating to the group of division directors are provided to the Governing Board. Directors having reason to ask the Administrator to prepare an individual report on a division director require the President's permission.

Reports on the Governing Board are provided to its members and to a Compliance and Integrity officer. If there is reason to ask the Administrator to prepare an individual report on a member of the Governing Board, the Compliance and Integrity officer is authorised to do so with the President's permission.

If the request for an individual report concerns the President of DNB, the Compliance and Integrity officer is authorised to submit the relevant request to the Administrator after obtaining the written permission of the Head of the Compliance and Integrity Department.

Article 8 Retention period
This Article provides that Personal Data logged in Monitoring the use of e-mail and the Internet are retained for a maximum period of six months within the framework of this Regulation.

Article 10 Rights of Employees
Article 10.3 refers to "special personal circumstances". These concern situations where the Employee's interests outweigh those of DNB in retaining the Employee's Personal Data. However, the Employee's right of correction does not extend to Log Data or Content Filtering, as this would impair the integrity of the systems. Objections may be submitted to the Compliance Officer. Handling objections is one of the responsibilities of the Secretary-Director, responsible for managing Internal Operations.

Article 11 Employees with a special status
The use of Digital Corporate Resources by the company doctor and the company welfare worker is not monitored within the framework of this Regulation.

The use of Digital Corporate Resources by members of the Works Council and appointed confidential advisers is monitored with extra care. This does not mean that Employees serving on the Works Council or appointed as confidential advisers are exempt from monitoring under this Regulation. Rather, it implies that they enjoy a protected status and are excluded from this Regulation to the extent that they use an e-mail account set up specifically for work relating to these duties (including ondernemingsraad@dnb.nl).