

DE NEDERLANDSCHE BANK N.V.

Regeling zorgvuldig omgaan met informatie

Artikel 1

In deze regeling wordt verstaan onder:

- a. *DNB*: De Nederlandsche Bank N.V.;
- b. *digitale bedrijfsmiddelen*: de door DNB aan de medewerker ter beschikking gestelde bedrijfsmiddelen waarop digitale informatie kan worden opgeslagen en faciliteiten voor de uitwisseling van informatie via digitale weg;
- c. *medewerker*: degene die werkzaam is ten behoeve van DNB;
- d. *informatie*: geheel van samenhangende gegevens, waaraan een bepaalde betekenis kan worden toegekend en waartoe de medewerker als gevolg van de uitoefening van zijn functie toegang tot heeft of krijgt.

Artikel 2

Deze regeling is van toepassing op alle medewerkers van DNB.

Artikel 3

Bij het omgaan met informatie houden medewerkers zich aan de geheimhoudingsverplichtingen voortvloeiende uit wetgeving, de CAO en de arbeidsovereenkomst.

Artikel 4

Bij het omgaan met informatie houden medewerkers zich aan de regelingen en instructies van DNB op het gebied van classificatie en beveiliging van informatie.

Artikel 5

Medewerkers delen informatie met elkaar als dit is toegestaan en als dit van belang is voor de uitoefening van hun taken en werkzaamheden.

Artikel 6

Medewerkers raadplegen informatie die niet aan hen is gericht slechts als deze informatie van belang is voor de uitoefening van hun taken en werkzaamheden.

Artikel 7

Medewerkers gebruiken informatie niet voor andere doeleinden dan de uitvoering van hun taken of werkzaamheden.

Artikel 8

- a. De wijze waarop medewerkers omgaan met informatie kan door DNB worden gecontroleerd.

- b. Voor informatie die toegankelijk is via digitale bedrijfsmiddelen is in de regeling 'Privacy bij controle gebruik digitale bedrijfsmiddelen' beschreven welke gegevens worden vastgelegd, op welke gronden de vastlegging plaatsvindt en op welke wijze en aan wie inzage wordt gegeven.

Toelichting bij de regeling zorgvuldig omgaan met informatie

Algemeen

DNB en haar medewerkers beschikken over veel vertrouwelijke informatie. In de Gedragscode DNB is vermeld dat medewerkers met deze informatie zorgvuldig omgaan en dat vertrouwelijke informatie vertrouwelijk wordt behandeld. Deze regeling beoogt de bepaling uit de Gedragscode DNB uit te werken.

De regeling bevat “principle based” voorschriften en gaat uit van de eigen verantwoordelijkheid van de medewerkers bij het omgaan met informatie. Doel van de regeling is om een kader te scheppen, waarbinnen de medewerker zijn eigen afweging dient te maken. In geval van twijfel dient de medewerker met zijn leidinggevende te overleggen.

Het door de regeling geschapen kader geldt voor alle medewerkers van DNB. De regeling heeft daarom voorrang boven voorafgaand aan de inwerkingtreding van de regeling gemaakte regels en afspraken, zowel op ‘bankbreed’ als op divisie- en afdelingsniveau. Divisies en afdelingen met eigen regels zullen deze derhalve na inwerkingtreding van onderhavige regeling moeten heroverwegen.

Artikelsgewijze toelichting

Artikel 1

Informatie

Het begrip informatie wordt ruim uitgelegd. Belangrijk is dat bij informatie niet alleen wordt bedoeld op gegevens die zijn vastgelegd op papier of op een informatiedrager (computer, memorstick); ook mondelinge informatie(bijvoorbeeld verkregen van een collega van een andere afdeling op een borrel binnen DNB) en informatie die zich in het geheugen van een persoon bevindt, vallen onder dit begrip en daarmee onder de reikwijdte van deze regeling.

Medewerker

Onder medewerker in de zin van deze regeling wordt iedereen verstaan die ten behoeve van DNB werkzaamheden verricht, onafhankelijk van de wijze waarop de relatie tussen DNB en deze persoon is vormgegeven. Bedoeld worden in ieder geval de medewerker met een vaste of tijdelijke aanstelling, de inhuurkracht, uitzendkracht, stagiaire of gedetacheerde. Er moet wel sprake zijn van enige vorm van een gezagsrelatie tussen DNB en de medewerker. Het gaat dus om werknemers en daarmee vergelijkbare medewerkers. Onafhankelijke externe adviseurs, maar ook dienstverleners als de glazenwassers, vallen derhalve niet onder de reikwijdte van deze regeling.

Artikel 3

De taken van DNB zijn gebaseerd op diverse wetten, die onder meer gemeenschappelijk hebben dat zij DNB en haar medewerkers tot geheimhouding verplichten. Uit de toezichtwetten, de Bankwet, de Statuten van DNB en de Statuten van het ESCB en de ECB vloeien wettelijke geheimhoudingsverplichtingen voort. Daarnaast voert DNB werkzaamheden uit die - ook zonder dat de wet daartoe verplicht - een vertrouwelijk karakter hebben.

In verband met de geldende geheimhoudingsverplichtingen ondertekenen medewerkers van DNB bij indiensttreding een geheimhoudingsverklaring, die deel uitmaakt van de arbeidsovereenkomst. De geheimhoudingsplicht van de medewerkers is niet gebonden aan een bepaalde soort informatie; zowel toezichtsinformatie, informatie afkomstig uit het ESCB als overige informatie met een vertrouwelijk karakter vallen onder deze plicht. De mate van vertrouwelijkheid van de informatie en de daaruit voortvloeiende geheimhoudingsverplichtingen zijn ook van invloed op de wijze waarop medewerkers onderling informatie mogen raadplegen en delen.

Artikel 4

Bij DNB wordt informatie geclassificeerd. Classificatie houdt in dat aan informatie een informatieklassering wordt toegekend, die de mate van vertrouwelijkheid van de informatie weergeeft. De informatieklassering geeft aan met wie de informatie (intern en extern) mag worden gedeeld.

Bij DNB bestaan voorts regelingen en instructies voor informatiebeveiliging die betrekking hebben op de wijze van opslag, verzending en vernietiging van informatie. De medewerker dient zich aan dergelijke interne regelingen en instructies te houden. Een voorbeeld van een dergelijke instructie is het clean desk principe, de brochure “Omgaan met vertrouwelijke informatie binnen en buiten DNB en de brochure “Informatie beveiligen en veilig internetten- Richtlijnen voor het gebruik van internet, e-mail en andere digitale middelen”.

Als bij bepaalde informatie de classificatie van de mate van vertrouwelijkheid ontbreekt, betekent dat zeker niet dat zonder meer aangenomen mag worden dat de informatie niet van vertrouwelijke aard is. Bij het ontbreken van kenbare classificatie zal de medewerker zich steeds een eigen oordeel moeten vormen omtrent de waarschijnlijke mate van vertrouwelijkheid ervan en daarnaar handelen. Bij twijfel omtrent de classificatie, is navraag geboden.

Artikelen 5,6 en 7

De artikelen 5 en 6 bepalen dat informatie mag worden gedeeld en geraadpleegd wanneer dit is toegestaan én wanneer dit van belang is voor het uitoefenen van taken en werkzaamheden. Daarnaast bepaalt artikel 7 dat informatie alleen mag worden gebruikt voor de doeleinden waarvoor de informatie is bestemd. Indien twijfels bestaan over de te hanteren norm, moet de medewerker met zijn leidinggevende bespreken hoe de norm dient te worden ingevuld. Hierna volgt enige uitleg over de begrippen ‘toegestaan’ en ‘van belang’, evenals een paar – niet limitatief bedoelde – voorbeelden van invulling van deze begrippen.

Toegestaan

Op basis van de aan de informatie toegekende informatieklassering kunnen medewerkers bepalen met wie bepaalde informatie mag worden gedeeld. Stukken die als ‘geheim’ zijn geclassificeerd, zijn bijvoorbeeld alleen bestemd voor de geadresseerden. De ontvanger van een dergelijk stuk mag deze informatie niet delen met anderen, ook wanneer de informatie bijvoorbeeld ‘handig’ zou kunnen zijn voor directe collega’s. Het delen van informatie is in een dergelijk geval dus niet toegestaan.

Van belang

Informatie die geclassificeerd is als vertrouwelijk mag in beginsel door een wijdere kring van medewerkers worden gedeeld en geraadpleegd. Voorwaarde is echter wel dat de informatie voor de ontvanger op enigerlei wijze van belang is voor de uitoefening van zijn taken of werkzaamheden. Het delen van informatie met collega’s enkel omdat het ‘leuk’ is iets te weten, valt dus niet in de categorie van belang voor de uitoefening van de taken en werkzaamheden. Ook

het bekijken van informatie vanwege een privébelang of persoonlijke interesse valt hier niet onder. Deze voorbeelden vallen in de categorie 'nice to know', terwijl met 'van belang' wordt bedoeld wat eerder wel werd aangeduid met de term 'need to know'.

Chinese walls

De regels over delen en raadplegen van informatie gelden ook wanneer medewerkers op basis van de toegekende informatieklassen of op grond van de Chinese walls toegang tot de informatie hebben of kunnen krijgen. Met het begrip Chinese walls worden de procedures en maatregelen aangeduid die regelen wie tot bepaalde informatie toegang heeft. Bepaalde medewerkers hebben uit hoofde van hun functie toegang tot een groot aantal dossiers en documenten. De bedoeling hiervan is uiteraard dat een medewerker beter zijn werk kan doen, wanneer hij toegang heeft tot alle informatie die hij voor zijn werk nodig heeft. De bedoeling is uitdrukkelijk niet dat medewerkers alle voor hen toegankelijke informatie 'zomaar' mogen bekijken.

De normen genoemd in de artikelen 5,6 en 7 zijn 'principle based' en geven daarom niet voor alle gevallen een exacte norm aan. Het is de eigen verantwoordelijkheid van de medewerker om – met inachtneming van de in deze regeling genoemde normen – een afweging te maken tussen wat is toegestaan en niet is toegestaan, welke informatie wél en welke niet van belang is. In geval van twijfel overlegt de medewerker met zijn leidinggevende of de compliance officer.