

DE NEDERLANDSCHE BANK N.V.

Regeling controle gebruik digitale bedrijfsmiddelen

Artikel 1 Definities

- a. *Beheerder*: de Medewerker die belast is met het beheer van een systeem of bedrijfsmiddel;
- b. *Contentfiltering*: het op geautomatiseerde wijze scannen en filteren van de inhoud van e-mails en het gebruik van internet van Medewerkers;
- c. *Controle*: toezicht door een manager op het gebruik van Digitale Bedrijfsmiddelen op basis van verkregen Rapportages;
- d. *Digitale Bedrijfsmiddelen*: de door DNB aan de Medewerker ter beschikking gestelde bedrijfsmiddelen waarop digitale informatie kan worden opgeslagen en geschikt is voor de uitwisseling van informatie via digitale weg;
- e. *DNB*: De Nederlandsche Bank N.V.;
- f. *Integriteitsschending*: een overtreding of een concreet vermoeden van een overtreding van interne dan wel externe wet- en regelgeving, waarbij de betrouwbaarheid van een Medewerker mogelijk in het geding is, als bedoeld in de Regeling bijzondere onderzoeken naar integriteitsschending;
- g. *Loggegevens*: de door middel van Logging verzamelde gegevens over het gebruik van Digitale Bedrijfsmiddelen;
- h. *Logging*: geautomatiseerde vastlegging van gegevens over het gebruik van Digitale Bedrijfsmiddelen;
- i. *Medewerker*: degene die werkzaam is ten behoeve van DNB;
- j. *Persoonsgegevens*: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;
- k. *Rapportage*: een geanonimiseerde rapportage die per sectie/afdeling/divisie wordt samengesteld op basis van Loggegevens en Contentfiltering;
- l. *Regeling*: onderhavige regeling welke ziet op Controle van Digitale Bedrijfsmiddelen;
- m. *Verkeersgegevens*: gegevens over gedrag van Medewerkers met betrekking tot het gebruik van Digitale Bedrijfsmiddelen, die niet de details van de berichten of bestanden betreffen;
- n. *Wbp*: de Wet bescherming persoonsgegevens.

Artikel 2 Reikwijdte

1. De Regeling is uitsluitend van toepassing op de controle van Digitale Bedrijfsmiddelen.
2. Indien een Integriteitsschending wordt vermoed, treedt de Regeling bijzondere onderzoeken naar integriteitsschending in werking.

Artikel 3 Controle

1. Controle in het kader van de Regeling vindt plaats op basis van een Rapportage.
2. Een Rapportage bevat slechts Verkeersgegevens.
3. Een Rapportage is in beginsel niet herleidbaar tot individuele Medewerkers.

Artikel 4 Doel van het controleren van de Digitale Bedrijfsmiddelen

1. Het controleren van het gebruik van de Digitale Bedrijfsmiddelen vindt slechts plaats in het kader van één of meer van de volgende doelen:
 - a. het toezicht op de naleving van interne regelingen van DNB;
 - b. het voorkomen van Integriteitsschendingen;
 - c. de beveiliging van de systemen en netwerken van DNB;
 - d. de bescherming van vertrouwelijke informatie van DNB;
 - e. de bescherming van de goede reputatie van DNB;
 - f. het verschaffen van managementinformatie in verband met de beheersing van kosten en capaciteit.
2. Bij de Controle worden de beginselen van proportionaliteit en subsidiariteit in acht genomen.

Artikel 5 Logging

1. Het gebruik van Digitale Bedrijfsmiddelen wordt gelogd.

2. De Loggegevens zijn uitsluitend toegankelijk voor de hiertoe geautoriseerde Beheerders.

Artikel 6 Rapportages

1. Op basis van Loggegevens en Contentfiltering kan de Beheerder periodiek of eenmalig geaggregeerde Rapportages genereren die betrekking hebben op een bepaald bedrijfsmiddel. Geaggregeerde Rapportages bevatten getotaliseerde gegevens en zijn geanonimiseerd. Geaggregeerde Rapportages worden verstrekt aan sectiehoofden, afdelingshoofden en (divisie)directeuren.
2. Indien een sectiehoofd, afdelingshoofd of divisiedirecteur op basis van een geaggregeerde Rapportage vermoedt dat het gebruik van een Digitaal Bedrijfsmiddel in strijd is met de Regeling, dan kan hij of zij de Beheerder verzoeken om een rapportage per individuele Medewerker. Voor het opvragen van een individuele rapportage heeft de manager, die voornemens is om een dergelijk verzoek neer te leggen bij de Beheerder, de toestemming nodig van zijn/ haar eigen manager. De betrokken Medewerker wordt zo spoedig mogelijk achteraf geïnformeerd van het feit dat een individuele rapportage is verstrekt.
3. 3.Individuele rapportages bevatten Verkeersgegevens die direct herleidbaar zijn tot individuele Medewerkers.

Artikel 7 Wet bescherming persoonsgegevens

Verwerking van Persoonsgegevens in het kader van deze regeling geschiedt in overeenstemming met de eisen die de Wbp (en overige relevante wetgeving) daaraan stelt.

Artikel 8 Bewaartermijn

1. Het resultaat van Logging en Contentfiltering wordt maximaal 6 maanden bewaard.
2. Gegevens worden zo spoedig mogelijk omgezet in Rapportages.
3. Persoonsgegevens die worden verwerkt in het kader van de Controle worden niet langer bewaard dan noodzakelijk. DNB hanteert daarbij een maximum bewaartermijn van zes maanden.

Artikel 9 Geheimhouding

Iedere Medewerker is verplicht tot geheimhouding van Persoonsgegevens waarvan hij of zij in het kader van deze regeling kennis heeft genomen, behoudens voor zover enig wettelijk voorschrift hem tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

Artikel 10 Rechten van de Medewerkers

1. De Medewerker kan zich tot de compliance officer wenden met het verzoek om een overzicht van zijn Persoonsgegevens die in het kader van deze regeling zijn vastgelegd in te zien of hierover informatie te ontvangen. Het verzoek wordt binnen vier weken beantwoord.
2. De Medewerker kan de compliance officer verzoeken zijn Persoonsgegevens te verbeteren, aan te vullen, te verwijderen indien deze feitelijk onjuist zijn, voor het doel onvolledig of niet terzake dienend, dan wel in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek wordt binnen vier weken beantwoord.
3. De Medewerker kan bij de compliance officer verzet aantekenen tegen de verwerking van zijn Persoonsgegevens in verband met bijzondere persoonlijke omstandigheden. De directie boordeelt binnen vier weken na ontvangst van het verzet of het verzet gerechtvaardigd is. Indien het verzet gerechtvaardigd is, beëindigt de Beheerder terstond de betreffende verwerking van de Persoonsgegevens.

Artikel 11 Medewerkers met een bijzondere status

Bij de Controle van het gebruik van de Digitale Bedrijfsmiddelen van de leden van de ondernemingsraad, de bedrijfsarts en overige medewerkers met een door de directie aangewezen vertrouwensfunctie wordt extra zorgvuldigheid in acht genomen.

Artikel 12 Klachten

1. Een Medewerker die van mening is dat door DNB in strijd is gehandeld met deze regeling dan wel anderszins in het kader van deze regeling een klacht heeft, wendt zich tot zijn direct leidinggevende.
2. Indien in overleg met de leidinggevende geen oplossing voor de klacht van de Medewerker kan worden gevonden, kan de Medewerker zich wenden tot de Klachtencommissie in de zin van de Algemene interne klachtenprocedure.

Toelichting bij de Regeling

Inleiding

DNB wil inzicht kunnen hebben in de wijze waarop Medewerkers de aan hen ter beschikking gestelde (Digitale) Bedrijfsmiddelen gebruiken. Een van de manieren om dit inzicht te verkrijgen is het op automatische wijze vastleggen van bepaalde gebruiksgegevens, ook wel loggen genoemd, en het controleren van deze gegevens. Deze Regeling geeft aan hoe DNB omgaat met de Controle van het gebruik van Digitale Bedrijfsmiddelen door haar Medewerkers en bepaalt de grenzen waarbinnen DNB mag opereren.

Een dergelijke Controle raakt de privacy van de Medewerkers. Daarom wordt in deze regeling een goede balans nagestreefd tussen het belang van DNB om het gebruik van Digitale Bedrijfsmiddelen te controleren en het belang van de Medewerkers bij bescherming van hun privacy. DNB handelt bij het controleren van de Medewerkers in lijn met de eisen die de Wbp (en eventueel overige toepasselijke wetgeving) daaraan stelt.

Artikelsgewijze toelichting

Artikel 1 Definities

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 de persoon die voor DNB werkzaamheden verricht op basis van een detacheringsovereenkomst. Er moet wel sprake zijn van enige vorm van een gezagsverhouding tussen DNB en de Medewerker. Het gaat dus om werknemers en daaraan gelijk te stellen medewerkers.

Bedrijfsmiddelen

Met bedrijfsmiddelen worden in algemene zin bedoeld 'de middelen en faciliteiten van DNB die door de Medewerker worden gebruikt bij de uitoefening van zijn werkzaamheden, evenals overige zaken die bij DNB aanwezig zijn', zoals bedoeld in de Regeling gebruik bedrijfsmiddelen. Bedrijfsmiddelen zijn dus computers, maar ook tafels, stoelen en papier.

Deze Regeling heeft alleen betrekking op het controleren van het gebruik van Digitale Bedrijfsmiddelen. De definitie van Digitale Bedrijfsmiddelen luidt: 'de door DNB aan de Medewerker ter beschikking gestelde bedrijfsmiddelen waarop digitale informatie kan worden opgeslagen en geschikt is voor de uitwisseling van informatie via digitale weg'.

Momenteel vallen onder dit begrip in ieder geval internet op de werkplek, e-mail, telefoon op de werkplek, het digitale archiefsysteem, de zoekmachine, de mobiele telefoon, de blackberry en de netwerkschijven.

Verder wordt opgemerkt dat het controleren zich ook kan uitstrekken tot het gebruik van Digitale Bedrijfsmiddelen voor het opslaan of verwerken van vertrouwelijke informatie in een cloud die niet door DNB ter beschikking is gesteld. Let wel, de opsomming uit de vorige alinea is niet limitatief. Onder de definitie van Digitaal Bedrijfsmiddel in de zin van deze Regeling vallen niet het tijdregistratiesysteem van DNB (TRS) en de toegangsregistratie. Alle Medewerkers van DNB zijn bekend met de interne regelingen en nadere instructies die bestaan omtrent het zorgvuldig omgaan met de ter beschikking gestelde bedrijfsmiddelen en de vertrouwelijke informatie. Die regels strekken zich ook uit tot opslaan/verwerken van vertrouwelijke gegevens in een cloud die niet door DNB ter beschikking is gesteld.

Let wel, de opsomming uit de vorige alinea is niet limitatief. Onder de definitie van Digitaal Bedrijfsmiddel in de zin van deze Regeling vallen bijvoorbeeld niet het tijdregistratiesysteem van DNB (TRS) en de toegangsregistratie.

Alle Medewerkers van DNB zijn bekend met de regels die bestaan omtrent het correct omgaan met vertrouwelijke informatie.

Persoonsgegevens

Voor wat betreft de definitie van Persoonsgegevens, sluit de Regeling aan op de definitie van Persoonsgegevens als opgenomen in artikel 1 van de Wbp. Dat houdt zoveel in dat alle gegevens die informatie kunnen verschaffen over een geïdentificeerde of identificeerbare natuurlijke persoon, Persoonsgegevens zijn. Ook gegevens die indirect identificerend zijn vallen hieronder; hiervan is bijvoorbeeld sprake wanneer gegevens zijn geanonimiseerd, maar in combinatie met andere gegevens kunnen worden teruggebracht tot een persoon.

Verkeersgegevens

Verkeersgegevens betreffen onder meer duur, aantal en tijdstip van het gebruik van Digitale Bedrijfsmiddelen. Voor zover het e-mail en internet berichten betreft wordt de inhoud daarvan door middel van Contentfiltering geautomatiseerd gescand of e-mailberichten bepaalde trefwoorden bevatten, of dat bezochte websites bepaalde trefwoorden bevatten. Indien een e-mailbericht een bepaald trefwoord bevat, dan wordt dat door Contentfiltering geautomatiseerd geregistreerd, en als een Verkeersgegeven opgenomen in een Rapportage.

Artikel 3 Controle

Controle vindt plaats op basis van Rapportages. De Rapportage is een overzicht dat in beginsel niet herleidbaar is tot een individueel persoon. Het doel van de Controle is welbepaald aangegeven in de Regeling.

Benadrukt wordt dat onderhavige Regeling met name is bedoeld om de manager de mogelijkheid te bieden om reeds in een vroeg stadium met zijn/haar sectie/afdeling/divisie in gesprek te gaan om duidelijk te maken dat mogelijk sprake is van gebruik van de Digitale Bedrijfsmiddelen in strijd met deze Regeling. De Medewerker die het aangaat wordt daarmee de gelegenheid geboden om het gebruik in strijd met onderhavige Regeling te staken.

Speciaal met het oog op het voorkomen van het (niet opzettelijk) uitlekken van bedrijfsgeheimen/ vertrouwelijke informatie wordt gebruik gemaakt van Contentfiltering. Dit houdt zoveel in dat door DNB zoektermen zijn geselecteerd die er op zouden kunnen wijzen dat informatie die mogelijk als bedrijfsgeheim/ vertrouwelijke informatie heeft te gelden, de organisatie verlaat. De Contentfiltering voor e-mailverkeer slaat alleen aan op het moment dat een e-mailbericht wordt verstuurd aan een niet-DNB adres, én een trefwoord bevat die zou kunnen duiden op de aanwezigheid van vertrouwelijke informatie/ van een bedrijfsgeheim.

Eenzijds wordt met de introductie van de Contentfiltering tegemoetgekomen aan het belang dat DNB heeft bij het voorkomen van het uitlekken van bedrijfsgeheimen/ vertrouwelijke informatie (w.o. toezichtvertrouwelijke informatie), en anderzijds wordt met de inzet van Contentfiltering een controlemiddel ingezet waarmee slechts een beperkte inbreuk op de privacy van de Medewerkers wordt gemaakt. Het na te streven doel kan niet worden bereikt door middel van de inzet van een 'lichter' instrument, waarbij zelfs gesteld kan worden dat de Contentfiltering een minder vergaande inbreuk vormt dan andere vormen van controle, zoals volledige inhoudscontrole of steekproefsgewijze inhoudscontrole.

Artikel 4 Doel van het controleren van de Digitale Bedrijfsmiddelen

De Wbp schrijft voor dat Persoonsgegevens slechts voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verkregen. De in het kader van deze Regeling verzamelde Persoonsgegevens mogen alleen worden verwerkt voor één of meer van de in artikel 4 genoemde doelen.

De Wbp schrijft voorts een proportionaliteit- en een subsidiariteitstoets voor. Een belangrijke toelichting kan gevonden worden in de toelichting op artikel 3 van de Regeling. Daarin werd al benadrukt dat een eerste stap die genomen kan worden door een manager, het informeren van de

sectie/ afdeling/ divisie dát er mogelijk sprake is van gebruik van de Digitale Bedrijfsmiddelen in strijd met de doelen van deze Regeling. Verder wordt benadrukt dat het controleren van het gebruik van Digitale Bedrijfsmiddelen met behulp van een Rapportage pas aan de orde komt wanneer andere maatregelen onvoldoende effectief zijn om de doelen als bedoeld in artikel 4 te bereiken (subsidiariteitsvereiste). Ook dient de wijze van Controle passend zijn voor het te bereiken doel en moet dit doel niet op andere wijze kunnen worden gerealiseerd (vereiste van proportionaliteit). Van belang is dat steeds aan deze vereisten wordt getoetst alvorens wordt besloten het gebruik van een bedrijfsmiddel op een bepaalde manier te controleren.

Met de in artikel 4 lid 1a genoemde interne regelingen van DNB wordt in hoofdzaak bedoeld op de Regeling gebruik bedrijfsmiddelen en de Regeling zorgvuldig omgaan met informatie.

Artikel 5 Logging

Het gebruik van Digitale Bedrijfsmiddelen wordt vastgelegd in een log. Dit betekent dat handelingen van de gebruiker met het betreffende bedrijfsmiddel worden geregistreerd op persoonsniveau. Een aantal voorbeelden hiervan zijn:

Gebruik mobiele communicatie en mobiel dataverkeer

Het gebruik van mobiele telefoon en mobiel dataverkeer wordt gelogd.

Gebruik van e-mail

Door middel van een Contentfiltering programma worden delen van Verkeersgegevens, de inhoud van e-mail berichten en de bijlagen, op basis van een set van trefwoorden gelogd die mogelijk vertrouwelijke informatie bevatten.

Gebruik van internet

Bezoek aan sites wordt geautomatiseerd gelogd. Door middel van een Contentfiltering programma wordt per Medewerker bijgehouden welke sites worden bezocht. Sites worden op basis van de inhoud ingedeeld in categorieën.

De logbestanden zijn uitsluitend te benaderen door geautoriseerde Beheerders die vanuit hun functie toegang dienen te hebben tot de logbestanden. De log wordt op geautomatiseerde wijze bijgehouden, dit betekent zonder menselijke tussenkomst.

Artikel 6 Rapportages

Van het gebruik van Digitale Bedrijfsmiddelen wordt een log bijgehouden. Op basis van Loggegevens en Contentfiltering kunnen Rapportages worden opgesteld. De Rapportage kan periodiek verstrekt worden aan het management ten behoeve van de Controle op gebruik Digitale Bedrijfsmiddelen.

Op dit moment wordt bijvoorbeeld van het gebruik van internet een niet tot individuele Medewerkers herleidbare Rapportage opgesteld, die maandelijks aan de afdelingshoofden, sectiehoofden en divisiedirecteuren wordt opgeleverd. De Rapportage ziet alleen op door Medewerkers bezochte websites in bepaalde ongewenste categorieën (zoals sex, gokken, etc). Deze Rapportage geeft dus geen inzicht in het totale internetgebruik van een Medewerker. Ook het gebruik van de mobiele communicatiemiddelen wordt standaard gerapporteerd. In dit geval wordt gerapporteerd over de duur en kosten van het gebruik van mobiele communicatiemiddelen in een bepaalde tijdsperiode en wordt wel per individuele Medewerker gerapporteerd. Deze kosten zijn relevant voor de organisatie die haar bedrijfsvoeringskosten wil bewaken.

Indien een manager op basis van een Rapportage vermoedt dat sprake is van ongeoorloofd gebruik van een bedrijfsmiddel heeft hij de mogelijkheid om de anonimiteit op te heffen. Let wel, dit houdt alleen in dat de rapportage ten aanzien van een bepaalde individuele Medewerker de Verkeersgegevens toont. Expliciet wordt gemeld dat *niet* de inhoud van berichten worden getoond. De individuele rapportage biedt de manager de mogelijkheid om de individuele medewerker aan te

spreken op het feit dat er op basis van de Verkeersgegevens aanwijzingen zijn van ongeoorloofd gebruik van de Digitale Bedrijfsmiddelen.

Een aanleiding om over te gaan tot een individuele rapportage kan bijvoorbeeld zijn dat uit de Rapportage een sterk afwijkend gebruik van een bepaald Digitaal Bedrijfsmiddel blijkt. De Beheerder stelt dan in opdracht van de manager, na toestemming van diens leidinggevende, een Rapportage op die herleidbaar is naar een individuele Medewerker.

Ook dan mogen, aldus lid 2 van dit artikel, alleen de Verkeersgegevens per individuele Medewerker worden gerapporteerd. Het verschil met de geaggregeerde Rapportage is dat deze wel op individueel niveau wordt gerapporteerd. In het kader van deze Regeling zal nooit de integrale inhoud van e-mailberichten, telefoongesprekken of via het internet uitgewisselde informatie of bestanden worden gerapporteerd. Controle van de integrale inhoud van berichten of bestanden etc is niet toegestaan in het kader van deze Regeling.

Bij een vermoeden van ongeoorloofd gebruik van Digitale Bedrijfsmiddelen hoeft het niet te gaan om een Integriteitsschending in de zin van de Regeling bijzondere onderzoeken naar Integriteitsschending. Indien bijvoorbeeld uit de Controle blijkt dat sprake is van bovenmatig privégebruik van bedrijfsmiddelen, of een andere overtreding van DNB regelgeving, kan de manager de betreffende Medewerker hierop aanspreken. Het is mogelijk dat de zaak hiermee is afgedaan. In gevallen waarin de Controle een concreet vermoeden bevat van een Integriteitsschending kan dit aanleiding geven melding te maken van een Integriteitsschending. Dit kan aanleiding zijn om een bijzonder onderzoek in het kader van de Regeling bijzondere onderzoeken naar Integriteitsschending te starten.

In onderhavige Regeling wordt gesproken over 'geanonimiseerde gegevens en anonieme gegevens'. Benadrukt wordt dat in dit kader niet wordt aangesloten bij de definitie die het College Bescherming Persoonsgegevens voor deze begrippen hanteert. In onderhavige regeling wordt met geanonimiseerde gegevens/ anonieme gegevens benadrukt dat het voor een manager in beginsel niet mogelijk is om op basis van de Rapportage te achterhalen welke Medewerker achter de Verkeersgegevens schuil gaat. Geanonimiseerde gegevens/ anonieme gegevens in het kader van onderhavige Regeling betekent expliciet niet dat het technisch onmogelijk is om een Medewerker aan een bepaalde hoeveelheid Verkeersgegevens te koppelen.

Artikel 6 lid 2 bepaalt dat het verzoek aan de Beheerder, strekkende tot het opvragen van een individuele rapportage, alleen ingewilligd wordt indien de manager die het verzoek doet ook toestemming heeft van zijn/ haar eigen manager. Daarbij wordt opgemerkt dat de Rapportage aangaande de groep van divisiedirecteuren aan de directie wordt gestuurd. Indien een directielid aanleiding ziet om een verzoek te doen aan de Beheerder om een individuele rapportage op te stellen over een divisiedirecteur, dan zal de directeur toestemming moeten hebben van de president van DNB.

De Rapportage van de directie wordt toegestuurd aan de directie én aan een medewerker van de afdeling Compliance en Integriteit. Indien aanleiding bestaat om een verzoek te doen aan de Beheerder om een individuele rapportage op te stellen over een directielid, dan zal de medewerker van de afdeling Compliance en Integriteit met instemming van de president van DNB, daartoe de bevoegdheid hebben.

Indien het verzoek strekkende tot een individuele rapportage, een individuele rapportage van de president van DNB betreft, dan heeft de medewerker van de afdeling Compliance en Integriteit de bevoegdheid om een verzoek aan de Beheerder te doen nadat schriftelijke toestemming van het afdelingshoofd van Compliance en Integriteit is gegeven.

Artikel 8 Bewaartermijn

Dit artikel ziet erop dat de Persoonsgegevens die worden gelogd in het kader van gebruik van e-mail en internet, maximaal zes maanden worden bewaard in het kader van deze Regeling.

Artikel 10 Rechten van de medewerkers

Artikel 10 lid 3 spreekt van bijzondere persoonlijke omstandigheden. Het moet hierbij gaan om belangen van de Medewerker die zwaarder wegen dat het belang van DNB bij het bewaren van de Persoonsgegevens. Het correctierecht van de Medewerker strekt zich echter niet uit tot de Loggings en Contentfiltering, omdat dit de integriteit van de systemen zou aantasten. Verzet kan worden aangetekend bij de compliance officer. Behandeling van het verzet valt onder de verantwoordelijkheid van de directeur intern bedrijf.

Artikel 11 Medewerkers met een bijzondere status

In het kader van onderhavige Regeling zal geen sprake zijn van het controleren van het gebruik van Digitale Bedrijfsmiddelen van de bedrijfsarts en de bedrijfsmaatschappelijk hulpverlener.

Voorts wordt opgemerkt dat de Controle van het gebruik van de Digitale Bedrijfsmiddelen van de ondernemingsraad en aangestelde vertrouwenspersonen met extra zorgvuldigheid wordt uitgevoerd. Dit betekent niet dat de Medewerkers die zitting hebben in de ondernemingsraad of aangesteld zijn als vertrouwenspersonen niet kunnen worden gecontroleerd in het kader van deze Regeling. Wél betekent dit dat de Medewerkers van de ondernemingsraad en de vertrouwenspersonen een beschermd status genieten en worden uitgezonderd van deze Regeling voor zover zij gebruik maken van een speciaal voor de met deze taken verbonden werkzaamheden ingerichte e-mailaccount. (waaronder: ondernemingsraad@dnb.nl).