De omgang met voorwetenschap door beursgenoteerde ondernemingen – Best Practices

Update mei 2021 – insiderlijsten en toegang tot voorwetenschap

De Autoriteit Financiële Markten (AFM) vindt het belangrijk dat ondernemingen die financiële instrumenten hebben uitgegeven die aan een beurs zijn genoteerd, blijvend aandacht besteden aan de omgang met voorwetenschap. Eind 2015 heeft de AFM een marktbrede inventarisatie uitgevoerd naar het proces van opstellen, publicatie en verspreiding van voorwetenschap door beursgenoteerde ondernemingen. Het doel van de inventarisatie was om meer inzicht te krijgen in de wijze waarop de persberichten worden opgesteld, hoe de persberichten worden verspreid en hoe de vertrouwelijkheid van voorwetenschap tot aan het moment van publicatie is gewaarborgd. Een bijzonder aandachtspunt hierbij was de samenwerking met externe organisaties. Deze inventarisatie heeft geresulteerd in de publicatie van best practices. Eind 2018 heeft de AFM opnieuw een verkenning bij beursgenoteerde ondernemingen uitgevoerd met het oog op de risico's van cybercriminaliteit bij het vertrouwelijk houden van voorwetenschap, zowel binnen de eigen organisatie als bij de organisaties waarmee voorwetenschap wordt gedeeld. Naar aanleiding van deze tweede inventarisatie heeft de AFM een ge-update versie van de best practices gepubliceerd in april 2019.

Update 2021

In 2020 heeft de AFM een verkenning uitgevoerd naar de omgang met voorwetenschap die zich heeft toegespitst op het volledig en actueel hebben en houden van insiderlijsten. Ook is gevraagd in welke mate beursgenoteerde ondernemingen, en organisaties waarmee zij samenwerken, inzicht hebben in wie wanneer toegang heeft tot voorwetenschap en waar die toegang uit bestaat (lezen, bewerken of

verwijderen van informatie). Naar aanleiding van deze laatste verkenning publiceert de AFM een bijgewerkte versie van de best practices. Er zijn drie onderwerpen toegevoegd: het samenstellen van de insiderlijst, toegang tot voorwetenschap en samenwerking met derden. Deze paragrafen staan aangeduid met 'update 2021'. De best practices bevatten op zichzelf geen (nieuwe) regels maar vormen voorbeelden en tips uit de dagelijkse praktijk die uw organisatie kunnen helpen om relevante procedures te toetsen of aan te scherpen. Tot slot merkt de AFM op dat dit document naast de best practices ook verwijzingen naar bestaande wettelijke verplichtingen bevat. Dit document geeft geen uitputtend overzicht van alle wettelijke verplichtingen en prevaleert ook niet boven wet- en regelgeving. Voor meer informatie over de omgang met voorwetenschap verwijst de AFM naar de geldende wet- en regelgeving en de verschillende brochures op de website van de AFM ten aanzien van omgang met en openbaarmaking van voorwetenschap.

Het vertrouwelijk houden van voorwetenschap

- **Beveilig uw voorwetenschap altijd goed,** bijvoorbeeld door het op te stellen en te bewaren in een afgeschermde digitale omgeving, door de inhoud te versleutelen of het document te beveiligen met een degelijk wachtwoord.
- **Vermijd het onbeveiligd verspreiden** van voorwetenschap, bijvoorbeeld per e-mail, zowel intern als extern. Dit geldt ook voor conceptversies.
- **Houd procedures en trainingen over omgang met voorwetenschap up-to-date.** Zorg voor procedures en houd regelmatig trainingen met uw medewerkers over de omgang met voorwetenschap binnen uw organisatie.
- **Neem voldoende maatregelen om de vertrouwelijkheid van voorwetenschap te waarborgen en toets de effectiviteit van deze maatregelen** (d.m.v. pen-testen, audits, etc.). Neem toereikende procedurele, technische en organisatorische maatregelen om de vertrouwelijkheid van voorwetenschap te garanderen. Laat uw cyberweerbaarheid periodiek testen door een externe partij. Draag er zorg voor dat u de toereikendheid van dergelijke maatregelen bij externe organisaties kent. Maak een afweging of de externe organisatie voldoende maatregelen heeft getroffen om uw voorwetenschap te mogen verwerken.
- **Bewustzijn over een langere periode.** In sommige gevallen kan voorwetenschap over een langere periode tot stand komen of zich steeds verder ontwikkelen (bijvoorbeeld tijdens overnamegesprekken). Zorg er in dergelijke situaties voor dat het bewustzijn met betrekking tot de omgang met voorwetenschap gedurende de hele periode punt van aandacht blijft, en niet alleen aan het begin of het eind van het proces. U kunt iemand aanwijzen (bijvoorbeeld uw compliance officer) die tijdens het gehele proces de

vertrouwelijke omgang met voorwetenschap bewaakt. Het gaat er hierbij om dat iemand verantwoordelijk wordt gemaakt die de centrale coördinatie voor zijn rekening neemt en die het onderwerp onder de aandacht blijft brengen door bijvoorbeeld het versturen van reminders, maar ook door het onderwerp te agenderen tijdens besprekingen. Ook kan de kennis hierover op peil worden gehouden door presentaties of trainingen.

- **Het belang van een volledige insiderlijst.** Zorg voor een complete insiderlijst en gebruik de template zoals opgenomen in de bijlagen uit de uitvoeringsverordening (EU) 2016/347. Hierop horen alle personen die in contact komen met voorwetenschap te worden vermeld, ook ondersteunende medewerkers (bijvoorbeeld het secretariaat of de postkamer). Het is verplicht om de insiderlijst continu actueel te houden. De AFM kan de insiderlijst opvragen. Indien veel externe partijen, zoals adviseurs, bekend zijn met de voorwetenschap dan is het voor de uitgevende instelling van belang om ook bij deze externe partijen te benadrukken dat het noodzakelijk is om zicht te hebben en te houden op de totale groep aan insiders (ook als deze mensen niet meer bij de voorwetenschap zijn betrokken). Alleen zo kan de uitgevende instelling de vertrouwelijkheid waarborgen.
- **Geheimhoudingsverklaring**. Laat uw medewerkers een geheimhoudingsverklaring en een gedragscode ondertekenen. Indien u een externe organisatie inschakelt om een persbericht te schrijven, te vertalen of (bijvoorbeeld juridisch) te beoordelen, leg geheimhouding dan contractueel vast.
- **Monitoring van media.** Monitor niet alleen de handel op de beurs als u de publicatie van voorwetenschap heeft uitgesteld. Volg de berichtgeving over uw onderneming (ook op social media) om aanwijzingen voor eventueel gelekte voorwetenschap te kunnen signaleren. Zorg altijd dat er een noodpersbericht klaar staat voor publicatie.
- **Contact met de AFM.** Neem bij incidenten, zoals bij het vermoeden dat voorwetenschap is gelekt, direct contact op met het monitoringteam van de AFM op 020-7973777.

Samenstellen van de insiderlijst (update 2021)

- **Maak een bewuste afweging over wie wel over de voorwetenschap wordt geïnformeerd en wie niet.** Daarmee wordt ook de keuze gemaakt wie er wel of niet op de insiderlijst komt te staan. De reden waarom iemand voorwetenschap heeft en wordt opgenomen op de insiderlijst, moet expliciet op de insiderlijst worden beschreven naast het vermelden van zijn of haar functietitel en rol. Consistentie over hoe die afweging binnen de gehele organisatie plaatsvindt, is hierbij van belang. De insiderlijst moet een volledig beeld geven van de personen die van de voorwetenschap op de hoogte zijn, zonder dat het aantal betrokkenen onnodig uitgebreid is. Wees er ook alert op dat personen die onderdeel uitmaken van

beslisorganen en uit dien hoofde worden geïnformeerd, ook worden opgenomen op de insiderlijst.

- **Bij de omgang met voorwetenschap is menselijk gedrag een belangrijke factor.** Hoe goed voorwetenschap technisch en procedureel is beveiligd, het waarborgen van de vertrouwelijkheid is afhankelijk van hoe mensen hiermee omgaan. Doorlopende aandacht voor het menselijke gedrag en een goede balans tussen hard en soft controls is dan ook noodzakelijk. Voorbeeldgedrag binnen een onderneming speelt hier ook een belangrijke rol bij. Maak medewerkers bewust van hoe ze moeten handelen in situaties waarin onverhoopt vertrouwelijke informatie toch is gedeeld.
- **Automatische koppelingen maken de kans kleiner op incorrecte of onvolledige insider lijsten.** Een automatische koppeling tussen de insiderlijst en bijvoorbeeld een autorisatie-, HR- of billingsysteem maakt de kans kleiner dat een insider niet op de insiderlijst wordt geplaatst of dat de persoonsgegevens van een insider incorrect of onvolledig op de insiderlijst worden overgenomen. Geef iemand pas toegang tot voorwetenschap nadat deze persoon op de insiderlijst is gezet. Andersom kan iemand ook automatisch op een insiderlijst worden opgenomen op het moment dat deze persoon digitale toegang krijgt tot de voorwetenschap.
- **Automatisering helpt om de administratieve tijdsbesteding te beperken.** Zorg dat alle documenten die betrekking hebben op of kwalificeren als voorwetenschap overzichtelijk op één plaats of in één systeem te vinden zijn. Wanneer gebruik wordt gemaakt van softwaretools van een externe partij voor het vastleggen van de insiderlijst, zorg er dan voor dat wordt voorkomen dat externe partijen toegang hebben tot de voorwetenschap. Waar dit niet te voorkomen is in verband met technische assistentie, zorg er dan voor dat ook de personen van de externe partij die toegang hebben tot de voorwetenschap op de insiderlijst komen te staan.
- **Inzicht en bewustzijn insiders.** Het draagt bij aan een bewuste omgang met voorwetenschap wanneer de aanmelding op de insiderlijst of het tekenen voor geheimhouding van informatie geen snelle ‘vink’ of ‘klik’ is. Ook helpt het als insiders binnen hun eigen onderneming weten welke andere personen insider zijn, zodat zij weten met wie zij kunnen spreken over de bij hen bekende voorwetenschap en met wie niet.
- **Maak één persoon (eind)verantwoordelijk.** Uit ervaringen van marktpartijen komt naar voren dat het goed werkt om één persoon eindverantwoordelijk te maken voor de volledigheid van de insiderlijst. Die persoon moet inzicht hebben in welke personen op welk moment op de hoogte zijn van de voorwetenschap, ook als deze personen zich op verschillende afdelingen of in verschillende beslisgremia bevinden. Uiteraard is het belangrijk om achtervang te hebben voor de eindverantwoordelijke.

- **ICT-kennis bij de teams die de insiderlijsten bijhouden is belangrijk.** Het ICT-proces is een integraal onderdeel van het proces van de omgang met voorwetenschap. Zorg ervoor dat de werknemers die de vertrouwelijke omgang met voorwetenschap bewaken ook beschikken over toereikende kennis van de ICT-processen en informatiebeveiliging.
- **Verhouding MAR en AVG.** De wettelijke verplichtingen ten aanzien van insiderlijsten uit de Verordening marktmisbruik (MAR) en de Algemene verordening gegevensbescherming (AVG) bestaan naast elkaar en hoeven elkaar niet in de weg te staan. Een praktisch voorbeeld van het naleven van beide verplichtingen is wanneer persoonsgegevens van het overzicht met de insiders gescheiden wordt gehouden, maar op een dusdanige manier dat er eenvoudig een koppeling met die persoonsgegevens kan worden gemaakt op het moment dat een toezichthouder de insiderlijst opvraagt.

Toegang tot voorwetenschap (update 2021)

- **Zorg ervoor dat er doorlopend goed inzicht is in welke personen op welke datum en welk tijdstip toegang tot de voorwetenschap hebben gehad en waar die toegang uit bestond (lezen, wijzigen of verwijderen van informatie).** Door (handmatig of geautomatiseerd) te monitoren wie daadwerkelijk toegang tot de voorwetenschap hebben, kan tijdens de omgang met voorwetenschap worden bewaakt dat er geen onbevoegden toegang hebben. Ook zorgt dit ervoor dat kan worden gecontroleerd dat de juiste personen op de insiderlijst staan.
- **Bevestig dat alle gebruikers (intern, extern en tijdelijk) en hun activiteiten op de ICT-systemen identificeerbaar en traceerbaar zijn**. Zorg er ook voor dat alle activiteiten van privileged accounts[1], zoals die van systeembeheerders, met betrekking tot de voorwetenschap geïdentificeerd en gemonitord worden.
- **Verleen toegangsrechten in lijn met de functie- en procesvereisten.** Zorg ervoor dat personen alleen toegang hebben tot die informatie en ICT-systemen die nodig zijn voor het uitvoeren van hun taak.
- **Monitor en verbeter voortdurend het controlekader[2] voor het proces inzake de omgang met voorwetenschap om de procesdoelstellingen te behalen**. Informatiebeveiliging (IB) is een integraal onderdeel van het proces inzake de omgang met voorwetenschap. Het is van belang om de effectiviteit van de maatregelen periodiek te testen, ook in combinatie met de overige

[1] Privileged access betreft alle accounts met meer toegangsrechten dan een standaardgebruiker. Voorbeelden van menselijke privileged access accounts zijn superusers zoals systeembeheerders, domeinbeheerders en lokale administrators. Een voorbeeld van de niet-menselijke privileged gebruikers is de applicatie-account om applicaties te beheren en aan te sturen. Misbruik van privileged accounts ligt veelal aan de basis van cyber-aanvallen.

[2] Het doel van een controlekader is om op organisatieniveau de beheersmaatregelen vast te leggen die minimaal benodigd zijn om op de diverse thema's (toegangscontrole, logging & monitoring) te kunnen voldoen aan de gestelde eisen.

IB-maatregelen die door de onderneming zijn genomen. Om het controlekader effectief te laten zijn moeten bevindingen binnen de onderneming worden gecommuniceerd en worden opgevolgd.

- **Het periodiek evalueren van het proces inzake de omgang met voorwetenschap is van belang.** Dit zorgt ervoor dat kan worden beoordeeld of er kwetsbaarheden in het proces bestaan en er of verbeteringen nodig zijn.

Samenwerking met derden (update 2021)

- **Wettelijke verplichting voor uitgevende instelling en derden.** Als een beursgenoteerde onderneming met externe adviseurs samenwerkt, zoals accountants, juridisch adviseurs, financieel adviseurs of consultants, is het van belang te realiseren dat het opstellen en bijhouden van de insiderlijst een wettelijke verplichting is voor zowel de uitgevende instelling als de personen die namens hen of voor hun rekening handelen. Dit is een verplichting die volgt uit de MAR. Het is van belang dat onderling duidelijk over en weer wordt gecommuniceerd dat er sprake is van voorwetenschap en welke verantwoordelijkheden daarbij horen.
- **Afspraken over informatiebeveiliging.** Op basis van inzicht in ketenafhankelijkheden streeft de onderneming ernaar afspraken te maken over informatiebeveiliging met andere partijen waarmee wordt samengewerkt. Dit betreft onder meer afspraken om de impact van incidenten, zoals ongeoorloofde toegang tot de voorwetenschap, te beperken voor zowel de getroffen onderneming als de gehele keten. Leg de afspraken hierover vast, bijvoorbeeld via non disclosure agreements (NDA's).

Het opstellen van een persbericht met voorwetenschap

- **Benoem een 'disclosure committee'.** Benoem een vaste kleine groep collega's die verantwoordelijk is voor de omgang met en de openbaarmaking van voorwetenschap. Het 'disclosure committee' komt bijeen om vast te stellen in hoeverre informatie als voorwetenschap kwalificeert, om de inhoud van persberichten met voorwetenschap te bespreken, het moment van publicatie te bepalen en eventueel uitstel van publicatie van voorwetenschap te documenteren. Zo'n 'disclosure committee' komt zowel periodiek als ad-hoc bijeen en bestaat uit medewerkers (bijvoorbeeld een lid van de Raad van Bestuur, een medewerker van de afdeling JZ, IR en Communicatie) die allen op de insider lijst van uw organisatie staan.

De publicatie en distributie van een persbericht met voorwetenschap

- **Voorwetenschap dient u zo snel mogelijk openbaar te maken.** Dat kan ook tijdens beursuren. De verplichting tot het zo snel mogelijk publiceren van voorwetenschap prevaleert ten opzichte van het nut om persberichten voor- of nabeurs te publiceren.
- **U blijft zelf verantwoordelijk voor het zo snel mogelijk openbaar maken en distribueren van voorwetenschap bij ingeschakelde externe organisaties.** De tijd tussen verzending van voorwetenschap aan derden die zijn ingeschakeld voor de distributie van uw persberichten en het moment van het door deze externe organisaties versturen aan de media moet zo kort mogelijk worden gehouden. U dient hier dus heldere afspraken over te maken met de externe organisatie. Zorg er bij het maken van afspraken ook voor dat het duidelijk is wie de contactpersonen zijn. Denk hierbij ook aan beschikbaarheid buiten kantooruren.
- **Maak enkel gebruik van gespecialiseerde bureaus.** Indien u gebruik maakt van derden voor de publicatie en distributie van uw persberichten, gebruik dan een organisatie die hierin is gespecialiseerd en die u bijvoorbeeld een beveiligd platform kan aanbieden waar u uw persbericht kunt uploaden en automatisch op een door uzelf vastgesteld tijdstip tegelijkertijd aan diverse media kunt laten distribueren.
- **U blijft verantwoordelijk voor de vertrouwelijkheid van de voorwetenschap, ook wanneer u voorwetenschap deelt met een externe organisatie.** Bedenk in hoeverre het echt noodzakelijk is om voorwetenschap met externe organisaties te delen. Wanneer dat het geval is, vertrouw dan niet alleen op de naam of professionaliteit van de externe organisatie, maar bespreek en leg contractueel vast hoe de vertrouwelijke en zorgvuldige omgang met voorwetenschap door de ingeschakelde externe organisatie is gewaarborgd. Communiceer over voorwetenschap alleen op een beveiligde manier, bij voorkeur minstens met 2-factor authenticatie of via een beveiligde portal. Houd voorwetenschap versleuteld totdat het wordt gepubliceerd. Maak afspraken over de verspreiding van voorwetenschap binnen externe organisaties. Ook bij hen dient de groep van personen die bekend raakt met voorwetenschap zo beperkt mogelijk te worden gehouden en moeten de personen op een insiderlijst staan.
- **Ga zorgvuldig om met het klaarzetten van persberichten met voorwetenschap.** Maak in communicatie over het persbericht met externe bureaus of andere adviseurs eerst gebruik van codes (zoals ‘XXX’) voor bijvoorbeeld belangrijke cijfers of bedrijfsnamen en vul deze pas in zodra het persbericht klaar is voor publicatie. Zet het persbericht niet alvast klaar op uw website voordat u het gaat publiceren, maar upload het persbericht pas op het allerlaatste moment op uw website en in het distributiesysteem. Het deponeren van

uw persberichten bij de AFM is pas toegestaan nadat het persbericht openbaar is gemaakt.

Disclaimer: deze best practices hebben een informatief doel. U kunt er geen rechten aan ontlenen. Als de tekst van de best practices afwijkt van de tekst en toelichting van wetgeving, dan gaat de wetgeving voor.