Praktijknotitie

Van: NOAB Adviesgroeplid WVO advocaten
Datum: april 2026
Categorie: arbeidsrecht
Onderwerp: Geheimhouding door werknemers van bedrijfsgevoelige informatie

1. Inleiding

Hoe houd je in de huidige digitale wereld jouw bedrijfsgevoelige informatie nog geheim? Met alle technologische ontwikkelingen en mogelijkheden zijn de 'papieren dossiers' inmiddels grotendeels verleden tijd. In plaats daarvan sturen we e-mails in plaats van brieven en leggen we documentatie veelal vast in computers. Ook de komst van Artificial Intelligence (hierna: "AI") heeft steeds meer invloed op het uitvoeren van de werkzaamheden. Van een simpele zoekopdracht tot het schrijven van teksten: AI wordt steeds vaker ingezet door werknemers. Dat biedt kansen, maar brengt ook risico's met zich mee voor werkgevers.

Het risico dat bedrijfsgevoelige informatie bij derden terecht komt, wordt steeds groter. Als werkgever wil je voorkomen dat werknemers vertrouwelijke informatie delen met derden. Het geheimhoudingsbeding mag daarom niet ontbreken in de arbeidsovereenkomst. Vaak is hier ook een boetebeding aan gekoppeld. Desalniettemin komt het voor dat bedrijfsgevoelige informatie en gegevens vanuit de (beveiligde) werkomgeving op de verkeerde plek terechtkomt. Vooral nu het werkende leven zich in bepaalde sectoren grotendeels digitaal afspeelt, zien we dat dit steeds vaker voorkomt. Hoe ga je in deze tijd nog om met de verplichting van werknemers om vertrouwelijke zaken en bedrijfsgevoelige informatie geheim te houden?

2. Bedrijfsgevoelige informatie / bedrijfsgeheimen

Eerst even terug naar de kern. Wat is een bedrijfsgevoelige informatie?

2.1. Definitie bedrijfsgevoelige informatie

2.2.1 Wettelijke herkomst definitie bedrijfsgevoelige informatie

De juridische oorsprong van de definitie van bedrijfsgevoelige informatie ligt in de zogenaamde TRIPS-overeenkomst[1] (de overeenkomst inzake handelsaspecten van de intellectuele eigendom). Hierin staan bepalingen over de bescherming van niet-openbaar gemaakte informatie, zijnde informatie die 1. geheim is, 2. handelswaarde bezit omdat deze informatie geheim is en 3. is onderworpen aan redelijke maatregelen om deze informatie geheim te houden.

Naast deze TRIPS-overeenkomst is door de Europese rechter geoordeeld dat bedrijfsgevoelige informatie of bedrijfsgeheimen alle niet-publieke informatie betreft die door het delen met derden tot schade kan leiden bij degene van wie de informatie afkomstig is.[2]

[1] Agreement on Trade-Related Aspects of Intellectual Property Rights, zie Trb. 1995, 130, Bijlage 1C.
[2] Het Gerecht 18 september 1996, T-353/94, ECLI:EU:T:1996:119, rov. 87 (Postbank/EC)

2.2.2. Definitie volgens de Wet bescherming bedrijfsgeheimen

Uiteindelijk hebben de TRIPS-overeenkomst en Europese rechtspraak de basis gevormd voor de Europese richtlijn bedrijfsgeheimen.[3] Deze richtlijn is in Nederland omgezet in de Wet bescherming bedrijfsgeheimen, de 'Wbb'. Volgens artikel 1 Wbb is bepaalde informatie een bedrijfsgeheim als die informatie aan drie cumulatieve voorwaarden voldoet. De informatie moet:

a. *geheim zijn*: daarbij is bepalend of de informatie eenvoudig toegankelijk is voor personen binnen de kringen die zich gewoonlijk met die informatie bezighouden. Alledaagse informatie is niet als geheim aan te merken;
b. *handelswaarde hebben omdat zij geheim is*: dit gaat om zowel feitelijke als potentiële handelswaarde; en
c. *onderworpen zijn aan redelijke maatregelen om deze geheim te houden*: Hierbij kan worden gedacht aan maatregelen zoals opnemen van geheimhoudingsbedingen, het expliciet benoemen of registreren van bedrijfsgeheimen, het bewaken van het bedrijfsterrein of de betrokken installatie dan wel digitale beschermingsmaatregelen.

2.2.3. Tussenconclusie definitie bedrijfsgeheimen

Er valt dus heel veel informatie onder het begrip bedrijfsgeheim: te denken valt aan knowhow, bedrijfsinformatie over bijvoorbeeld klanten/projecten/investeringen en technologische informatie. Voldoet het aan bovenstaande criteria, dan is het een bedrijfsgeheim. Nb: in het vervolg wordt met bedrijfsgeheim ook bedrijfsgevoelige informatie bedoeld en visa versa.

3. Arbeidsrechtelijke aspecten geheimhouding van bedrijfsgevoelige informatie

Om bedrijfsgeheimen te beschermen heeft een werkgever verschillende arbeidsrechtelijke mogelijkheden. Te denken valt aan het overeenkomen van een geheimhoudingsbeding en het wettelijke instructierecht van de werkgever zoals opgenomen in artikel 7:660 BW. Ook kan een beroep worden gedaan op het vereiste van de werknemer zich als een goed werknemer te gedragen (artikel 7:611 BW). In deze paragraaf gaan we de verschillende mogelijkheden langs. In paragraaf 4 worden de sanctiemogelijkheden behandeld.

3.1. Geheimhoudingsbeding

De meest bekende vorm om bedrijfsgevoelige informatie te beschermen is het geheimhoudingsbeding. Deze staat vaak in de arbeidsovereenkomst, maar dat hoeft niet. Er is geen wettelijke definitie van het geheimhoudingsbeding. Uit rechtspraak volgt dat de strekking van een geheimhoudingsbeding in het algemeen is: '*het beschermen van de vennootschap en de daarbij behorende belanghebbenden tegen het weglekken van vertrouwelijke en concurrentiegevoelige informatie, vanwege de daaraan verbonden zakelijke risico's.*'.[4] Een geheimhoudingsbeding geeft een werkgever dus de mogelijkheid om zijn bedrijfsgevoelige informatie te beschermen.

Hoe effectief een geheimhoudingsbeding is, hangt af van de formulering van het geheimhoudingsbeding. Indien er in enige mate onduidelijkheid is over de reikwijdte van het beding, dan wordt deze uitge-

[3] Richtlijn (EU) 2016/943 van het Europees Parlement en de Raad van 8 juni 2016 betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan;
[4] Gerechtshof Arnhem-Leeuwarden, 23-08-2016, ECLI:NL:GHARL:2016:6750

legd aan de hand van de 'Haviltex-maatstaf'. Dat houdt in dat wordt gekeken naar de zin die partijen in de gegeven omstandigheden over en weer redelijkerwijs aan deze bepaling mochten toekennen en op hetgeen zij te dien aanzien redelijkerwijs van elkaar mochten verwachten. Simpeler omschreven: de letterlijke tekst is niet alleen bepalend, het gaat er ook om wat partijen ermee hebben bedoeld en wat zij daarin hebben verwacht of mochten verwachten dat de andere partij heeft bedoeld. Indien het geheimhoudingsbeding voor meerdere soorten uitleg vatbaar is, wordt uitgegaan van de uitleg die voor de werknemer het gunstigste is. Vandaar dat een onzorgvuldig geformuleerd geheimhoudingsbeding nadelige gevolgen kan hebben voor een werkgever.[5]

Je kunt het beste duidelijke en heldere taal kan gebruiken in de formulering van het geheimhoudingsbeding. Dit kan bijvoorbeeld door zoveel mogelijk letterlijk op te schrijven wat wel en niet is toegestaan. Daarmee voorkom je dat werkgever en werknemer andere bedoelingen hebben of een andere bedoeling hadden verwacht. Uit rechtspraak volgt namelijk dat een te algemeen of beperkt geformuleerd geheimhoudingsbeding niet effectief is. Een werkgever zal bij discussie dan sneller ongelijk krijgen.

3.1.1. Rechtspraak formulering geheimhoudingsbeding

Stel, een werknemer stuurt bedrijfsgevoelige informatie naar zijn privé-e-mailadres. Er is dan geen sprake van een overtreding van het geheimhoudingsbeding als in het beding slechts is opgenomen dat het delen van informatie met derden niet is toegestaan.[6] De werknemer deelt de informatie namelijk met zichzelf en dus niet met derden. Het is daarom beter om op te nemen dat het '*op welke wijze dan ook buiten de macht brengen*' van bedrijfsgevoelige informatie niet is toestaan. De formulering van het geheimhoudingsbeding is nog beter als in de tekst staat dat ook het brengen, op welke wijze dan ook, van bedrijfsgevoelige informatie naar de privéomgeving van werknemer niet is toegestaan.[7] Zo oordeelde de kantonrechter Amsterdam dat het sturen van vertrouwelijke informatie naar het prive-e-mailadres een schending van het geheimhoudingsbeding was omdat in het geheimhoudingsbeding expliciet stond dat dit verboden was.[8]

3.2. Instructierecht

Naast het geheimhoudingsbeding kan een werkgever gebruik maken van het instructierecht ex artikel 7:660 BW. Dit instructierecht biedt de mogelijkheid om kaders te stellen rondom het gebruik en het delen van bedrijfsgevoelige informatie. Artikel 7:660 BW bepaalt dat '*de werknemer, binnen de grenzen van algemeen verbindende voorschriften en/of de arbeidsovereenkomst, verplicht is zich te houden aan voorschriften die door of namens de werkgever worden gegeven omtrent het verrichten van de arbeid en/of welke strekken ter bevordering van de goede orde in de onderneming van de werkgever*'. Dat is veel tekst, maar in essentie komt het erop neer dat als werkgever werkinstructies en ordevoorschriften kunt geven.

In het belang van de goede orde in de onderneming kan een werkgever via het instructierecht de werknemer bijvoorbeeld verbieden om bedrijfsgevoelige informatie buiten de macht van de werkgever te brengen. Een werkgever doet er dan verstandig aan om ook te definiëren wat 'buiten de macht van

[5] Gerechtshof Arnhem-Leeuwarden, 23-08-2016, ECLI:NL:GHARL:2016:6750 , r.o. 5.3
[6] Hof Den Haag 15 november 2016, ECLI:NL:GHDHA:2016:3313, rov. 2.11; Gerechtshof Arnhem-Leeuwarden 15 januari 2019, ECLI:NL:GHARL:2019:287, rov. 4.1; Gerechtshof Den Haag 8 februari 2022, ECLI:NL:GHDHA:2022:343, rov. 5.19; Gerechtshof Arnhem-Leeuwarden 22 maart 2022, ECLI:NL:GHARL:2022:2248, rov. 3.6 en Rechtbank Midden-Nederland 13 april 2023, ECLI:NL:RBMNE:2023:1814, rov. 5.9.
[7] Zie bijvoorbeeld: Rechtbank Amsterdam 6 april 2023, ECLI:NL:RBAMS:2023:2056 & Rechtbank Noord-Holland 5 januari 2022, ECLI:NL:RBNHO:2022:180
[8] Rechtbank Amsterdam 6 april 2023, ECLI:NL:RBAMS:2023:2056

werkgever' betekent. Op die manier maakt de werkgever duidelijk wat wel en niet mag. Een werkgever kan dus ook via dit instructierecht verbieden dat werknemers bedrijfsinformatie gebruiken op persoonlijke apparaten of invoeren in een AI-tool. Een uitwerking van zo'n instructie is het opstellen en hanteren van beleid. Er kan natuurlijk ook sprake zijn van een ad hoc instructie via een e-mail waarbij is aangegeven dat dit geheime informatie is.

3.2.1. Rechtspraak beleid en instructie werkgever

Uit de rechtspraak volgt dat het van groot belang is dat dit beleid/de instructie bekend is bij werknemers en dat dit in de praktijk consistent wordt nageleefd en gehandhaafd door de werkgever. Alleen dan kan een werkgever een geslaagd beroep doen op het beleid/de instructie. Kortom, het beleid mag niet willekeurig worden toegepast anders verliest het aan kracht en werking.

Zo werd een werknemer terecht op staande voet ontslagen nadat hij in strijd met de gedragscode van werkgever bestanden opstelde en naar zijn privé-e-mailadres stuurde waarin bedrijfsgevoelige informatie over (klanten van) werkgever stond.[9] Ook een werknemer die op non-actief was gesteld en desondanks in strijd met aanwezig beleid bedrijfsgevoelige informatie naar verschillende externe e-mailadressen stuurde, werd terecht op staande voet ontslagen. Hierbij woog ook mee dat de werknemer in het kader van hoor- en wederhoor geen deugdelijke verklaring had voor zijn actie. De stelling dat werknemer de informatie nodig had als verweer in zijn ontslagprocedure werd niet gevolgd door de rechter.[10]

3.3. Het begrip goed werknemerschap

Naast een geheimhoudingsbeding en duidelijk intern beleid over omgang met bedrijfsgevoelige informatie, kan een werkgever zich nog beroepen op het beginsel van 'goed werknemerschap' (artikel 7:611 BW). Van een goed werknemer wordt immers verwacht dat hij zorgvuldig omgaat met bedrijfsgevoelige informatie. Gaat hij niet zorgvuldig om met bedrijfsgevoelige informatie, dan schendt de werknemer de wettelijke plicht om zich ten opzichte van zijn werkgever als goed werknemer te gedragen.[11] Deze schending kan vervolgens de grondslag zijn om een schadevergoeding te vorderen. De mogelijkheden voor het vorderen van een schadevergoeding wordt verder besproken in paragraaf 4.2.

4. Arbeidsrechtelijke sancties en gevolgen

Er zijn dus verschillende arbeidsrechtelijke mogelijkheden die een werkgever kan gebruiken om de bedrijfsgevoelige informatie te beschermen. Het is raadzaam om bij die mogelijkheden ook sanctiemogelijkheden op te nemen. Op die manier is het vooraf bekend bij werknemer wat de gevolgen van overtredingen zijn. Er zijn verschillende sanctiemogelijkheden. Een werkgever kan bijvoorbeeld een boetebeding koppelen aan een overtreding of aangeven dat - in een uiterst geval - ontslag het gevolg is van een overtreding.

4.1. Boetebeding

Artikel 7:650 BW geeft de mogelijkheid om boetes te stellen op overtredingen van voorschriften in de arbeidsovereenkomst. Het geheimhoudingsbeding in de arbeidsovereenkomst is zo'n voorschrift. Een boetebeding heeft in de eerste plaats een afschrikwekkende en daarmee tevens preventieve werking. De gedachte is dat werknemers wel twee keer nadenken voordat ze het geheimhoudingsbeding over-

[9] Rechtbank Noord-Holland 16 september 2025, ECLI:NL:RBNHO:2025:10627, r.o. 4.7 e.v..
[10] Gerechtshof Den Haag 24 november 2020, ECLI:NL:GHDHA:2020:2102
[11] Kamerstukken II 2017/18, 34821, nr. 3, blz. 3 (MvT bij Wbb)

treden. Het biedt de werkgever bovendien nog een ander voordeel; hij hoeft namelijk niet te stellen en te onderbouwen welke schade hij heeft geleden als gevolg van de overtreding.

Natuurlijk moet het boetebeding wel aan een aantal geldigheidsvereisten voldoen. Een boete op het geheimhoudingsbeding is bijvoorbeeld alleen geldig als deze ziet op dat geheimhoudingsbeding en schriftelijk overeen is gekomen. Daarnaast moeten de boetebedragen in het beding schriftelijk zijn vastgelegd, moet de bestemming van de boete zijn vermeld en mag het weektotaal aan boetebedragen in geval van een minimumloon niet hoger zijn dan een halve dag loon. Hiervan kan worden afgeweken als de werknemer meer verdient dan het minimumloon.

4.2. Schadevergoeding vorderen

Wanneer een werkgever schade leidt door het handelen van zijn werknemer gedurende de uitvoering van de werkzaamheden, is de werknemer in beginsel niet aansprakelijk. Dit is geregeld in artikel 7:661 BW. Een werknemer kan alleen aansprakelijk zijn als er sprake is van opzet of bewuste roekeloosheid. Van opzet of bewuste roekeloosheid is zelden sprake. De bewijslast ligt hier bij de werkgever. Dit betekent dat een werkgever moet aantonen dat er sprake is van opzettelijk handelen of bewuste roekeloosheid. Daarnaast moet een werkgever zo concreet mogelijk onderbouwen welke schade er is geleden door dit handelen van de werknemer.[12] Bij deze onderbouwing kun je denken aan:

i. de kosten van maatregelen ter verwijdering van de gegevens,
ii. (onderzoeks)kosten van adviseurs,
iii. Schade doordat de bedrijfsgevoelige informatie toegankelijk is geworden voor derde partijen of schade omdat je als werkgever niet meer kan beschikken over de bedrijfsgevoelige informatie,
iv. schade door vertrekkende relaties,
v. reputatieschade; en
vi. eventuele schade door een datalek.

4.2.1. Rechtspraak bij vorderen schadevergoeding

Een werknemer handelde bewust roekeloos door een grote hoeveelheid bedrijfsgevoelige informatie naar zijn privéaccount te sturen. Deze werknemer was op non-actief gesteld en er was kenbaar intern beleid aanwezig waarin stond dat dergelijk gedrag niet toelaatbaar was. In deze situatie kon werkgever daarom met succes de onderzoekskosten en andere kosten verhalen op de werknemer.[13]

In een recente zaak bij de rechtbank Overijssel ging het over onder andere het gebruik van AI en het presteren van de werknemer. De werkgever stelde dat de werknemer ondermaats presteerde omdat hij bijvoorbeeld zijn social media posts door AI liet schrijven. Daarvoor waren geen instructies bekend die ervoor zorgde dat de invoer van gegevens in een AI-tool en het gebruiken van AI in de werkzaamheden reguleerde. Deze werkgever voerde onvoldoende feiten en omstandigheden aan waaruit volgde dat werknemer bewust roekeloos handelde door onder andere het gebruik van AI. Ook was er onvoldoende onderbouwing van de door werkgever gestelde schade.[14]

Ook de vordering van een werkgever die de onderzoekskosten als schade wilde verhalen wegens het kopiëren en/of downloaden van bestanden door de werknemer was niet-succesvol. Hier downloadde de werknemer regelmatig bestanden en informatie naar de privé-laptop om zo te kunnen werken. Er was

[12] Rechtbank Overijssel 10. Maart 2026 ECLI:NL:RBOVE:2026:1328
[13] Gerechtshof Den Haag 23 maart 2021, ECLI:NL:GHDHA:2021:428 en HR 25 maart 2022, ECLI:NL:HR:2022:448. Zie ook de in paragraaf 3.2.1. genoemde uitspraak van Gerechtshof Den Haag 24 november 2020, ECLI:NL:GHDHA:2020:2102 waarin al werd geoordeeld dat deze werknemer terecht op staande voet was ontslagen.
[14] Rechtbank Overijssel 10 Maart 2026, ECLI:NL:RBOVE:2026:1328

namelijk geen bedrijfslaptop beschikbaar. Daarnaast had werknemer grote hoeveelheid bestanden gekopieerd ten behoeve van een ontslagprocedure. In die kwestie koppelde de rechter het oordeel over de aansprakelijkheid aan het handelen van werknemer. Dat handelen werd als niet ernstig verwijtbaar gezien, omdat het handelen gebruikelijk was en soms zelfs onvermijdelijk was ondanks aanwezig beleid waarin stond dat dit handelen niet was toegestaan.[15]

In het hoger beroep over voorgenoemde zaak is nog aanvullend geoordeeld dat er geen sprake was van bedrijfsgevoelige informatie zoals bedoeld in de Wbb (zie paragraaf 2.2.2.).[16] Zo was er discussie over de vraag of het ging om geheime informatie (ex artikel 1 sub 1 Wbb), of de bestanden ook handelswaarde bezaten (artikel 1 sub b Wbb) en of er redelijke maatregelen waren ter bescherming die de werknemer ook bekend waren (artikel 1 sub c Wbb).

4.3. Ontbinding ernstig verwijtbaar handelen (e-grond)

Behalve de bovengenoemde sancties boete en schadevergoeding, is er in sommige situaties ook ontslag mogelijk. Hierbij kan worden gedacht aan ontbinding wegens (ernstig) verwijtbaar handelen en ontslag op staande voet (zie paragraaf 4.4). Het gaat voor deze praktijknotitie te ver om ook diep in te gaan op het hele juridisch kader van (ernstig) verwijtbaar handelen.

Ontbinding wegens (ernstig) verwijtbaar handelen wordt over het algemeen gezien als alternatief voor ontslag op staande voet. Het verschil is echter wel dat je voor een ontbinding naar de kantonrechter moet. Voor een succesvol beroep op ontbinding wegens (ernstig) verwijtbaar handelen, moet de werkgever aantonen dat het handelen van werknemer dusdanig verwijtbaar is dat van een werkgever niet kan worden gevergd de arbeidsovereenkomst te laten voortduren. Voor de werknemer moet wel duidelijk zijn dat het handelen ontslag tot gevolg heeft, al dan niet op staande voet.

In zijn algemeenheid geldt dat schending van het geheimhoudingsbeding als verwijtbaar handelen wordt gezien.[17] Desondanks betekent dat niet direct dat het onrechtmatig downloaden van bedrijfsgevoelige informatie automatisch tot ontbinding leidt.[18] Het hangt nog steeds af van alle omstandigheden van het geval.

4.3.1. Rechtspraak bij ontbinding wegens ernstig verwijtbaar handelen

Ook op dit punt zijn enkele voorbeelden in de rechtspraak. Zo werd een arbeidsovereenkomst wegens ernstig verwijtbaar handelen niet ontbonden, omdat niet kwam vast te staan dat de gedownloade informatie bedrijfsgevoelig was.[19] Ook volgde er geen ontbinding in de situatie waarin werkgever niet kon aantonen dat de bedrijfsgevoelige informatie met derden was gedeeld.[20] Ontbinding kwam er evenmin in een situatie dat de werknemer via zijn persoonlijke elektronische apparaten toegang had tot de bedrijfsgevoelige gegevens. In deze situatie was werkgever daarvan vooraf op de hoogte.[21] Tot slot volgde er ook geen ontbinding in de situatie dat de werknemer de informatie had gedownload om zichzelf in rechte te kunnen verdedigen.[22]

---

[15] Rechtbank Rotterdam 9 oktober 2023, ECLI:NL:RBROT:2023:11880, r.o. 2.5, 2.6 & 2.9.
[16] Gerechtshof Den Haag 13 augustus 2024, ECLI:NL:GHDHA:2024:1455, r.o. 5.8
[17] M.A. Schneider, 'Kroniek e-grond', ArbeidsRecht 2022/43.
[18] A.J.A. Leemans & F.S. Sodenkamp, 'Keep it secret, keep it safe', ArbeidsRecht 2026/3.
[19] Rechtbank Overijssel 21 augustus 2020, ECLI:NL:RBOVE:2020:2820.
[20] Rechtbank Midden-Nederland 16 februari 2024, ECLI:NL:RBMNE:2024:1232
[21] Gerechtshof Den Haag 13 augustus 2024, ECLI:NL:GHDHA:2024:1455
[22] Rechtbank Midden- Nederland 16 februari 2024, ECLI:NL:RBMNE:2024:1232

4.4. Ontslag op staande voet

Tot slot bestaat de mogelijkheid om een werknemer op staande voet te ontslaan. In het arbeidsrecht wordt dit instrument gezien als laatste redmiddel. Het mag dan ook niet lichtzinnig worden gebruikt en er zijn strenge voorwaarden aan verbonden. Iemand verliest namelijk van de een op de andere dag zijn baan en heeft ook geen recht op een WW-uitkering. Het is dan ook geen zekerheid dat overtredingen van het geheimhoudingsbeding, instructies (lees: beleid) of goed werknemerschap automatisch leiden tot een rechtsgeldig ontslag op staande voet. Of een ontslag op staande voet rechtsgeldig kan worden gegeven hangt uiteindelijk af van alle omstandigheden van het geval. Het gaat voor deze praktijknotitie te ver om diep in te gaan op het exacte juridische kader bij ontslag op staande voet. Er vallen wel enkele lessen te halen uit de rechtspraak bij ontslag op staande voet.

4.4.1. Rechtspraak bij ontslag op staande voet

Er is bijvoorbeeld geen dringende reden voor ontslag op staande voet als de gedeelde informatie niet kwalificeert als bedrijfsgevoelige informatie.[23] Er is ook geen dringende reden als er geen redelijke maatregelen vooraf zijn genomen ter bescherming van de bedrijfsgevoelige informatie [24] of als de informatie is gedownload ter bescherming van de eigen rechtspositie.[25] De werknemer die niet meewerkte aan een verzoek tot verwijdering of teruggave van de bedrijfsgevoelige informatie die hij zelf buiten de macht van werkgever had gebracht werd wel terecht op staande voet ontslagen.[26]

5. Conclusies en aanbevelingen

Omgaan met de verplichting van werknemer om bedrijfsgevoelige informatie geheim te houden is gelukkig mogelijk. Er zijn arbeidsrechtelijke mogelijkheden die een werkgever kan gebruiken en er zijn sanctiemogelijkheden. De vervolgstap is dat een werkgever deze ook gaat gebruiken. Ik sluit daarom samenvattend af met een aantal aanbevelingen:

- Stel een zorgvuldig geformuleerd geheimhoudingsbeding op in de arbeidsovereenkomst en koppel daaraan een boetebeding;
- Gebruik de mogelijkheid om beleid op te stellen over hoe werknemers moeten omgaan met bedrijfsgevoelige informatie en wees in dat beleid duidelijk over de gevolgen (sancties) van overtredingen van dat beleid. Pas dit beleid ook consequent toe;
- Wees je bewust van de huidige ontwikkelingen dat werknemers gebruik (gaan) maken van AI. Als je al beleid hebt ten aanzien van het geheimhouden van bedrijfsgevoelige informatie, pas dat dan aan op AI-gebruik. Heb je geen beleid over geheimhouden van bedrijfsgevoelige informatie en AI-gebruik? Stel dat dan op of laat het opstellen;
- Win altijd juridisch advies in als je te maken krijgt met overtredingen van het geheimhoudingsbeding of je beleid hieromtrent. Het is namelijk belangrijk dat je de juiste stappen onderneemt bij het vorderen van een boete of schade of het inzetten van ontslag.

---

[23] Rechtbank Overijssel 11 juni 2021, ECLI:NL:RBOVE:2021:2468; Hof Arnhem- Leeuwarden 22 juni 2020, ECLI:NL:GHARL:2020:4724 en Rb. Rotterdam 31 mei 2024, ECLI:NL:RBROT:2024:5514.

[24] Rechtbank Haarlem 12 februari 2007, ECLI:NL:RBHAA:2007:AZ8506 en Gerechtshof Den Haag 13 december 2016, ECLI:NL:GHDHA:2016:3611.

[25] Rechtbank Limburg 21 maart 2017, ECLI:NL:RBLIM:2017:2517; Gerechtshof Amsterdam 17 november 2020, ECLI:NL:GHAMS:2020:3112; Rechtbank Midden-Nederland 16 augustus 2024, ECLI:NL:RBMNE:2024:5298 en Rechtbank Gelderland 24 oktober 2024, ECLI:NL:RBGEL:2024:6966

[26] Rechtbank Den Haag 24 februari 2023, ECLI:NL:RBDHA:2023:8545; Rechtbank Den Haag 28 september 2023, ECLI:NL:RBDHA:2023:21760 en Gerechtshof Den Haag 24 juli 2024, ECLI:NL:GHDHA:2024:1167

6. Ten slotte

Heb je vragen over de inhoud van deze NOAB praktijknotitie, dan kun je als NOAB-lid in het kader van de NOAB-helpdesk contact opnemen met:

NOAB Adviesgroeplid WVO Advocaten
Tel. 055-5066650

Voorwaarden en disclaimer

Deze praktijknotities zijn specifiek bedoeld voor NOAB-kantoren. Het is niet toegestaan deze te delen met andere partijen. Daarnaast is de disclaimer van kracht die je kunt vinden op https://noab.nl/disclaimer-privacy-en-cookieverklaring/.