HODARI
PRIVACY COMPLIANCE SECURITY GOVERNANCE

Passende organisatorische en technische maatregelen

A. (Afaaf) Al-Taher, L. (Lodewijk) Benjaminse en R. (Ruud) Buurma
januari 2020

OPENBAAR

Inleiding

1

1. Inleiding
2. Zaken
3. Analyse
4. Samenvatting
5. Bronvermelding

Inleiding
Achtergrond

In deze publicatie behandelen wij enkele onderzoeken en uitspraken van toezichthouders. De toezichthouders waren van mening dat organisaties onvoldoende *"passende technische en organisatorische maatregelen"* hadden genomen. HODARI houdt zich dagelijks bezig met deze combinatie van informatiebeveiliging en privacy en was voor ons daarom aanleiding om de onderbouwing van de toezichthouders op een rij te zetten om zo een beter beeld te krijgen bij de "*passende technische en organisatorische maatregelen*".

De zes zaken die wij in deze publicatie bespreken, zijn behandeld door de volgende toezichthouders binnen de EER: Autoriteit Persoonsgegevens (Nederland), Comissão Nacional de Protecção de Dados (Portugal) en Datatilsynet (Noorwegen).

In de zaken die wij hebben bekeken komen de volgende aspecten uit het vakgebied van informatiebeveiliging prominent naar voren:

- autorisatie;
- logging;
- authenticatie;
- bewustwording;
- datalekken.

Aan de hand van de zes zaken zullen wij voor deze vijf onderwerpen aangeven wat de overwegingen van de toezichthouder waren.

Zaken

2

1. Inleiding
2. Zaken
3. Analyse
4. Samenvatting
5. Bronvermelding

Zaken
Onvoldoende maatregelen

Hieronder introduceren wij de zes zaken waarbij de toezichthouder van mening was dat de betreffende organisaties onvoldoende "*passende technische en organisatorische maatregelen*"hadden genomen.

1. Zorgverzekeraar Menzis heeft februari 2018 een last onder dwangsom opgelegd gekregen van EUR 50.000. Menzis heeft tijdig aan de last voldaan en daarom heeft de Autoriteit Persoonsgegevens geen dwangsom ingevorderd. Daarmee zijn dit interessante besluiten die concrete handvatten biedt ten aanzien van informatiebeveiliging in het algemeen en in de zorgsector in het bijzonder.[2 7]

2. In april 2018 heeft Centro Hospitalar Barreiro Montijo (een ziekenhuis in Portugal) een aantal boetes van in totaal EUR 400.000 opgelegd gekregen van Comissão Nacional de Protecção de Dados (de Portugese toezichthouder) omdat het ziekenhuis er niet in was geslaagd de toegang tot persoonsgegevens van patiënten te beperken en de vertrouwelijkheid, integriteit en beschikbaarheid te waarborgen.[1 3 4]

3. Op 4 april 2018 werd bij de Autoriteit Persoonsgegevens gemeld dat er sprake was van een datalek bij het HagaZiekenhuis. Medische gegevens van een bekende Nederlandse waren ingezien door 85 werknemers van het ziekenhuis die niet direct betrokken waren bij de behandeling van deze patiënte, waardoor hun inzage in het digitale patiëntendossier een onrechtmatige verwerking was. Uit het onderzoek van de Autoriteit Persoonsgegevens bleek dat het ziekenhuis de informatiebeveiliging ten aanzien van persoonsgegevens van patiënten niet op orde had.[5]

Zaken
Onvoldoende maatregelen

4. In Noorwegen heeft Datatilsynet (de toezichthouder aldaar) maart 2019 aan de gemeente Bergen een boete EUR 170.000 opgelegd omdat wachtwoorden van 35.000 gebruikersnamen van voornamelijk leerlingen maar ook werknemers van scholen publiekelijk zichtbaar waren. Hierdoor was het mogelijk dat derden toegang kregen tot persoonsgegevens van deze leerlingen en werknemers. Op grond van artikel 5 lid 1 sub f en artikel 32 heeft de toezichthouder gemeend dat er onvoldoende "*passende technische en organisatorische maatregelen"* waren genomen.[6]

5. Eind september 2019 is een werknemer van het HagaZiekenhuis ontslagen, nadat hij een dienstoverdracht van de verpleegafdeling als boodschappenlijstjes had gebruikt en in een winkelkarretje in een supermarkt had achtergelaten. Hierdoor waren onder andere de namen, de geboortedata, medicatie en klachten van negentien patiënten zichtbaar. Deze gegevens werden vervolgens gevonden en zijn met de media gedeeld. De toezichthouder heeft het ziekenhuis een last onder dwangsom opgelegd, van EUR 100.000 per twee weken met een maximum van EUR 300.000. [8] [9] [10] [11]

6. Medewerkers van VGZ hebben toegang gehad tot medische gegevens, terwijl dit voor hun werkzaamheden niet noodzakelijk was. De Autoriteit Persoonsgegevens meende dat de technische maatregelen onvoldoende waren. Dit was voor de Autoriteit Persoonsgegevens een reden om VGZ een last onder dwangsom op te leggen. VGZ heeft tijdig aan de last voldaan. De toezichthouder heeft daarom bij VGZ geen dwangsom ingevorderd.[12] [13]

Analyse

3

1. Inleiding
2. Zaken
3. Analyse
4. Samenvatting
5. Bronvermelding

Analyse
Uitgangspunten

In de AVG zijn op verschillende plekken bepalingen over "*passende technische en organisatorische maatregelen*" opgenomen. Zo bepaalt artikel 32 lid 1 van de AVG dat verwerkingsverantwoordelijke en de verwerker *"passende technische en organisatorische maatregelen"* dienen te nemen *"om een op het risico afgestemd beveiligingsniveau te waarborgen"*. De volledige tekst van het betreffende artikel staat hier rechts weergegeven.

Bij het nemen van deze maatregelen moeten organisaties rekening houden met:
- de stand van de techniek;
- de uitvoeringskosten;
- de aard;
- de omvang;
- de context;
- de verwerkingsdoeleinden;
- de risico's voor de rechten en vrijheden van personen.

Daarnaast blijkt dat de toezichthouder in Nederland (de Autoriteit Persoonsgegevens) eveneens de UAVG (Uitvoeringswet Algemene verordening gegevensbescherming), NEN 7510 (Informatiebeveiliging in de zorg) en NEN 7513 (Logging: vastleggen van acties op elektronische patiëntdossiers) betrekt in haar overwegingen.

Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

a. de pseudonimisering en versleuteling van persoonsgegevens;

b. het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;

c. het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;

d. een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Analyse
Uitgangspunten

Aangezien de AVG buiten artikel 32 niet concreet aangeeft wat "*passend*" is, gaan wij aan de hand van de onderzoeken en uitspraken van de toezichthouders in op "*technische en organisatorische maatregelen*" waar zij naar verwijzen.

Deze maatregelen zijn binnen het vakgebied van de informatiebeveiliging thuis te brengen onder de volgende onderwerpen:

- autorisatie;
- authenticatie;
- logging;
- bewustwording;
- datalekken.

Wij mogen veronderstellen dat deze onderwerpen waar de toezichthouders zich op baseren, bekend waren bij de betreffende organisaties; zeker wanneer op dergelijke omvang (gevoelige) persoonsgegevens worden verwerkt.

Analyse
Autorisatie

- Het beleid gericht te zijn op profielen waarbij bevoegdheden worden gekoppeld aan de rol van een persoon: ook wel *role based access* genaamd. Artikel 9 lid 2 onder h en lid 3 van de AVG, artikel 30 lid 3 onder a en lid 4 van de UAVG en artikel 7:457 eerste en tweede lid Burgerlijk Wetboek bepalen dat alleen personen die wegens hun persoonsgegevens ambt, beroep of wettelijk voorschrift, dan wel krachtens een overeenkomst tot geheimhouding verplicht zijn, persoonsgegevens mogen verwerken. De bevoegdheden van een werknemer beschrijven tot welke informatie deze persoon toegang geeft en welke acties hij mag uitvoeren. Het HagaZiekenhuis beschikt over een autorisatiematrix, waarin is aangegeven dat enkel de persoonsgegevens van een patiënt waar de werknemer een behandelrelatie mee heeft toegankelijk zijn voor die werknemer. De bevoegdheden zijn tevens beperkt in tijd, namelijk voor de duur van één jaar om de werkzaamheden in het kader van de behandelrelatie af te ronden.

- Bij het onderzoek dat de toezichthouder bij VGZ heeft verricht, is gebleken dat sommige werknemers feitelijk wel toegang tot persoonsgegevens hadden, terwijl Menzis het organisatorisch zo had ingericht dat het niet mogelijk zou moeten zijn. Dit betekent dat onvoldoende passende technische maatregelen waren genomen conform artikel 32 van de AVG. De toezichthouder heeft daarom Menzis gelast om een autorisatiematrix op te stellen dat de bevoegdheden beschrijft die bij een rol horen. Hierbij dient Menzis vast te leggen voor welke rol het verwerken van persoonsgegevens betreffende de gezondheid noodzakelijk is en voor welk doeleinde. Voorts dienen in de systemen de bevoegdheden van werknemers van Menzis daarmee blijvend feitelijk in overeenstemming te worden gebracht.

Analyse
Autorisatie

- Het Portugese ziekenhuis had 985 gebruikers gekoppeld aan het 'medisch' profiel waarmee zij toegang hadden tot patiëntendossiers terwijl er maar 296 artsen werkzaam waren. (Sinds november 2016 waren er geen accounts meer geblokkeerd.) Ongeacht de specialisatie van de arts, was elke arts in staat persoonsgegevens in te zien van elke patiënt. Er was geen formele procedure die het aanmaken van accounts beschreef en tevens ontbrak een autorisatiematrix die de relatie tussen profielen en toegang tot persoonsgegevens beschreef.

  In de ogen van de toezichthouder heeft het ziekenhuis niet voldaan aan minimale gegevensverwerking zoals vermeld in artikel 5 lid 1 sub c van de AVG. Uit dit artikel blijkt namelijk dat persoonsgegevens toereikend moeten zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Door aan een buitensporig groot aantal gebruikers toegang te verlenen tot patiëntendossiers heeft de toezichthouder conform artikel 83 lid 5 sub a van de AVG geoordeeld dat een basisbeginsel inzake verwerking is geschonden.

  Ten tweede heeft de toezichthouder op grond van artikel 5 lid 1 sub f en artikel 83 lid 5 sub a van de AVG geoordeeld dat het ziekenhuis door gebrek aan *"technische en organisatorische maatregelen"* de vertrouwelijkheid en integriteit niet kon waarborgen.

  Als laatste meende de toezichthouder dat vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht zoals genoemd in artikel 32 lid 1 sub b niet werden gegarandeerd.

Analyse
Logging

- NEN 7510 (12.4.1 en 12.4.2) en NEN 7513 (5.1) geven aan dat logging moet worden gemaakt van "*gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen"* en informatie moet bevatten over de vraag "*wie toegang tot hun patiëntdossier hebben en hebben gehad"*. Deze logbestanden dienen te worden "*bewaard en regelmatig te worden beoordeeld" en "beschermd tegen vervalsing en onbevoegde toegang"*, zodat onweerlegbaar kan worden vastgesteld wie welke activiteiten heeft uitgevoerd. De Autoriteit Persoonsgegevens heeft vastgesteld dat het HagaZiekenhuis geen systematische, risicogerichte c.q. intelligente controle van de logging uitvoerde.

  De Autoriteit Persoonsgegevens geeft een aantal handvatten en is van mening dat:
  - enkel willekeurig steekproefsgewijs controleren op basis van klachten van slechts enkele dossiers niet voldoende is;
  - er sprake dient te zijn van controle van logging van alle dossiers door te selecteren op opvallende afwijkingen of uitschieters;
  - er sprake dient te zijn van automatische signaleringen bij overschrijding van bepaalde grenswaarden;
  - controle van logging van een aselecte steekproef van jaarlijks zes patiëntendossiers geen systematische, risicogerichte c.q. intelligente controle van de logging is;
  - gelet op de schaal van de organisatie de omvang van de controles voldoende moet zijn.

Analyse
Logging

- Bij Menzis en VGZ was geen logging aanwezig waarna de Autoriteit Persoonsgegevens oordeelde dat er geen passende technische maatregelen waren genomen. De toezichthouder heeft aangegeven dat zij door middel van logging van toegang en mutaties – al dan niet naar aanleiding van incidenten – kunnen controleren of medewerkers toegang hebben verkregen terwijl de toegang tot deze gegevens niet noodzakelijk is voor hun werkzaamheden.

Analyse
Authenticatie

- NEN 7510-2 bepaalt in 9.4.1 het volgende: *"Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, behoren de identiteit van gebruikers vast te stellen en dit behoort te worden gedaan door middel van authenticatie waarbij ten minste twee factoren betrokken worden."* Er dient dus sprake te zijn van minimaal twee factoren bij de authenticatie. Volgens de Autoriteit Persoonsgegevens voldeed het HagaZiekenhuis hier niet aan, want er kon worden ingelogd met enkel een wachtwoord.

- Persoonsgegevens moeten op een dusdanige manier worden verwerkt dat een passende beveiliging ervan is gewaarborgd en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging ("*integriteit en vertrouwelijkheid*"). Dit staat genoemd in artikel 5 lid 1 sub f van de AVG en werd volgens de toezichthouder niet door het Centro Hospitalar Barreiro Montijo nageleefd.

- Ook in Noorwegen was schending van dit artikel 5 lid 1 sub f van de AVG aanleiding om een boete op te leggen. Volgens de Noorse toezichthouder Datatilsynet had gemeente Bergen geen passende maatregelen genomen om de persoonlijke gegevens in haar systemen te beschermen. Op systemen van de gemeente stonden bestanden met gebruikersnamen en wachtwoorden van accounts die voor het grote publiek toegankelijk waren. Hierdoor was het voor iedereen mogelijk om met die gebruikersnamen en wachtwoorden in te loggen op systemen van de scholen en daarmee toegang te krijgen tot verschillende persoonsgegevens van leerlingen en werknemers van die scholen.

Analyse
Bewustwording

- NEN 7510 (7.2.2) bepaalt dat werknemers *"een passende bewustzijnsopleiding en -training behoren te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie"*. De gevolgen van het schenden van informatiebeveiliging en de disciplinaire processen zijn juist hierbij van belang. De Autoriteit Persoonsgegevens heeft vastgesteld dat het HagaZiekenhuis hieraan voldoet. Dit aangezien er workshops waren georganiseerd, informatie via intranet wordt gedeeld, aan een landelijke bewustzijnscampagne werd deelgenomen en een brief is verspreid over de normen en de mogelijke sancties na de melding van het datalek van de bekende Nederlandse patiënte.

Analyse
Datalekken

- Hoe *"technische en organisatorische maatregelen"* dienen te worden ingericht door zorgaanbieders is nader uitgewerkt in de normen NEN 7510 en NEN 7513. Zodra een (mogelijk) datalek heeft plaatsgevonden, dient door een organisatie zelf te worden nagegaan of alle passende technische en organisatorische maatregelen zijn genomen. De Autoriteit Persoonsgegevens heeft daarom de eisen uit NEN 7510 en NEN 7513 gehanteerd om te bepalen of de maatregelen van het HagaZiekenhuis passend zijn.

- Onbevoegde inzage door werknemers in persoonsgegevens over de gezondheid van patiënten is een voorbeeld van een datalek. Als het waarschijnlijk is dat de datalek tot een risico voor de rechten en vrijheden van natuurlijke personen leidt, dient deze aan de Autoriteit Persoonsgegevens te worden. Wanneer het waarschijnlijk is dat de inbreuk een hoog risico voor de rechten en vrijheden van natuurlijke personen met zich mee brengt, moet de datalek betrokkene te worden gemeld. Bij de beoordeling hiervan moet altijd gekeken worden naar de specifieke omstandigheden van het datalek en moet de vraag gesteld worden of de inbreuk wel of niet bewust of opzettelijk heeft plaatsgevonden. De AVG schrijft voor dat alle datalekken door de organisatie intern vastgelegd dienen te worden, ook die datalekken die uiteindelijk niet worden gemeld bij de Autoriteit Persoonsgegevens of de betrokkene. Daarnaast dient ook een passend beleid voor gegevensbescherming voor handen te zijn waarin staat wat er gedaan moet worden indien zich een datalek voordoet. De Autoriteit Persoonsgegevens heeft beoordeeld dat het HagaZiekenhuis de artikelen 24 lid 2, 33 en 34 van de AVG goed heeft nageleefd.

Samenvatting

4

1. Inleiding
2. Zaken
3. Analyse
4. Samenvatting
5. Bronvermelding

Samenvatting
Passende organisatorische en technische maatregelen

Door toezichthouders zijn afgelopen jaren op grond van de AVG in een aantal zaken een boete en/of een last onder dwangsom opgelegd omdat er onvoldoende *"passende technische en organisatorische maatregelen"* zouden zijn genomen. Wij hebben deze zaken in dit artikel besproken en gekeken welke aspecten de toezichthouder rondom *"passende technische en organisatorische maatregelen"* relevant acht.

Hieronder geven wij een samenvatting van de relevante *"passende technische en organisatorische maatregelen"* die organisaties in ogenschouw dienen te nemen. Dit betreft zowel het opstellen van beleid en procedures als de inrichting en naleving daarvan.

- **autorisaties:**
  De organisatie dient te beschikken over:
  - procedures rondom autorisaties;
  - bevoegdheden die feitelijk in lijn zijn met de rol van de werknemer (*role based access*) en daarmee de (eindige) relatie tot patiënt en zijn de betreffende persoonsgegevens;
    - autorisatiematrix *(soll)* dat de toegang tot persoonsgegevens en toegestane acties beschrijft (organisatorisch);
    - implementatie van autorisatiematrix in systemen (technisch) *(ist);*
  - procedure voor in-, door- en uitstroom van werknemers waarin het toekennen/intrekken van bevoegdheden en het aanmaken/blokkeren van accounts staan beschreven.

Op grond van de uitspraken, kunnen we concluderen dat deze onderwerpen relevant zijn om *"passende technische en organisatorische maatregelen"* te nemen:

- autorisatie;
- logging;
- authenticatie;
- bewustwording;
- datalekken.

Tot slot merken graag op dat (naast een eventuele boete of dwangsom door de toezichthouder) het ook mogelijk is dat een organisatie een schadevergoeding opgelegd krijgt op grond van artikel 82 van de AVG. De rechter oordeelde immers in mei 2019 dat *"door de verspreiding van [...] persoonsgegevens sprake is geweest van een schending van de privacy"*.[14]

Samenvatting
Passende organisatorische en technische maatregelen

- **logging:**
  De organisatie dient te beschikken over:
  - vastlegging, beoordeling en bescherming van logging van activiteiten.

- **authenticatie:**
  De organisatie dient te beschikken over:
  - twee factoren (bijvoorbeeld naast het wachtwoord ook een SMS, token, smartcard of app) tijdens de authenticatie daar waar het bijzondere persoonsgegevens van patiënten betreft;
  - opslag van wachtwoorden zodat deze niet herleidbaar zijn bijvoorbeeld door het correct toepassen van *hashing* en *salt.*

- **bewustwording:**
  De organisatie dient te beschikken over:
  - bewustwording van werknemers omtrent de risico's van informatiebeveiliging en privacy.

- **datalekken:**
  De organisatie dient te beschikken over:
  - adequaat beleid en passende procedures omtrent (het onderzoeken, melden, vastleggen, ... van) datalekken.

Bronvermelding

5

1. Inleiding
2. Zaken
3. Analyse
4. Samenvatting
5. Bronvermelding

Bronvermelding

1. "*Portuguese hospital appeals GDPR fine*", IT Governance, 15 oktober 2018, https://www.itgovernance.eu/blog/en/portuguese-hospital-appeals-gdpr-fine
2. "*Financieel jaarverslag 2018*", Coöperatie Menzis, 29 maart 2019, https://www.zorgictzorgen.nl/wp-content/uploads/2019/04/Jaarrekening-2018-Cooperatie-Menzis-UA.pdf
3. "*First GDPR fine in Portugal issued against hospital for three violations*", IAPP, 3 januari 2019, https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations
4. "*Hospital do Barreiro contesta judicialmente coima de 400 mil euros de Comissão de Dados*", Publico, 22 oktober 2018, https://www.publico.pt/2018/10/22/sociedade/noticia/hospital-barreiro-contesta-judicialmente-coima-400-mil-euros-comissao-dados-1848479
5. "*85 medewerkers Hagaziekenhuis berispt na inbreuk dossier Barbie*", NRC, 26 april 2018, https://www.nrc.nl/nieuws/2018/04/26/85-medewerkers-hagaziekenhuis-berispt-na-inbreuk-dossier-barbie-a1600992
6. "*Administrative fine of 170.000 € imposed on Bergen Municipality*", Datatilsynet, 4 december 2019, https://www.datatilsynet.no/en/regulations-and-tools/reports-on-specific-subjects/administrative-fine-of-170.000--imposed-on-bergen-municipality
7. "Last onder dwangsom en definitieve bevindingen", Autoriteit Persoonsgegevens, 15 februari 2018, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_last_onder_dwangsom_menzis.pdf
8. "*Gevoelige informatie van patiënten HagaZiekenhuis in boodschappenkarretje achtergelaten*", AD, 7 september 2019, https://www.ad.nl/den-haag/gevoelige-informatie-van-patienten-hagaziekenhuis-in-boodschappenkarretje-achtergelaten~a211434a

Bronvermelding

9. "*Negentien patiënten de dupe van lek in HagaZiekenhuis*", AD, 10 september 2019, https://www.ad.nl/den-haag/negentien-patienten-de-dupe-van-lek-in-hagaziekenhuis~ac7162b4
10. "Patiënten Haga-ziekenhuis ingelicht over uitlekken gegevens", NOS, 8 september 2019, https://nos.nl/artikel/2300875-patienten-haga-ziekenhuis-ingelicht-over-uitlekken-gegevens.html
11. Autoriteit Persoonsgegevens, 16 juli 2019, https://autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-pati%C3%ABntendossiers
12. "*Sancties voor Menzis en VGZ voor overtreding van de privacywet*", Autoriteit Persoonsgegevens, 4 november 2019, https://autoriteitpersoonsgegevens.nl/nl/nieuws/sancties-voor-menzis-en-vgz-voor-overtreding-van-de-privacywet
13. "*Last onder dwangsom en definitieve bevindingen*", Autoriteit Persoonsgegevens, 15 februari 2018, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_last_onder_dwangsom_vgz.pdf
14. ECLI:NL:RBOVE:2019:1827, Rechtbank Overijssel, 6 juni 2019, https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBOVE:2019:1827

HODARI
PRIVACY COMPLIANCE SECURITY GOVERNANCE

HODARI levert diensten op het gebied van security, privacy, governance, risk en compliance. Wij brengen IT op orde door risico's in informatiebeveiliging te beperken en wij helpen organisaties aantoonbaar in control te komen. Wij bieden kwalitatief hoogwaardige oplossingen waarbij de meest complexe vraagstukken tot in detail zijn opgelost. Wij hebben ruime ervaring opgedaan binnen verschillende sectoren, zoals de financiële sector, energiesector, (rijks)overheid, advocatuur, IT-dienstverleners en retail. Regelmatig handelen wij binnen projecten naar aanleiding van fusies en overnames, reorganisaties, bevindingen van accountants of opmerkingen van toezichthouders.

HODARI B.V.

071-2032385
hodari.nl

L. (Lodewijk) Benjaminse
lodewijk.benjaminse@hodari.nl