



Infodoc

Veilig omgaan met informatie

Versie: November 2019



Inhoudsopgave

Veilig omgaan met informatie	3
Privacy en Security Team	3
Verwerking van persoonsgegevens	4
Informatiebeveiliging	4
Bol Adviseurs mailt veilig	5
Voorwaarden veilig omgaan met informatie	5
Vragen?	8
Bijlage 1: Certificaat ISO 27001	9

Veilig omgaan met informatie

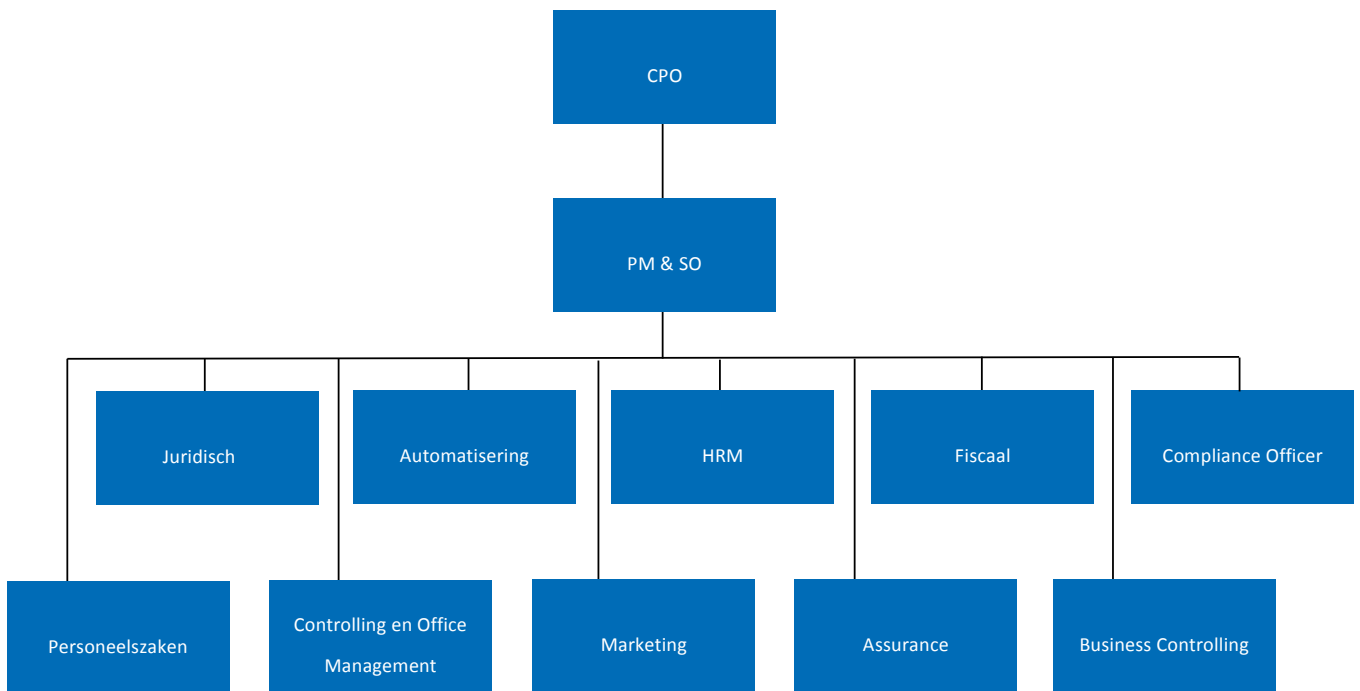
Bol Adviseurs hecht veel waarde aan het veilig omgaan met informatie. Alleen een bewustwordingsprogramma, een virusscanner of een wachtwoordprocedure is niet voldoende. De keten is zo sterk als de zwakste schakel. Daarom past Bol Adviseurs haar beveiligingsmaatregelen toe op mens, organisatie en techniek. In dit infodoc lees je hoe Bol Adviseurs hier invulling aan geeft.

Privacy en Security Team

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. Bol Adviseurs hecht veel waarde aan de naleving van deze verordening. Vraagstukken op het gebied van privacy en security worden behandeld door het Privacy en Security Team, ook wel PST genoemd. Het PST bestaat uit een kernteam en medewerkers van de diverse afdelingen van Bol Adviseurs. Het kernteam wordt gevormd door:

- Chief Privacy Officer (CPO): Roy Verbroekken MSc CBC RA, partner
- Privacy manager (PM): Thijs Peeters MSc EMITA CIPP/E, IT Auditor
- Security Officer (SO): Ruud Hofmans S-ISME, IT Manager

Het PST wordt als volgt weergegeven:



Het PST behandelt interne vraagstukken van medewerkers en externe vraagstukken van klanten en betrokkenen. Wil je contact opnemen met het PST? Stuur dan een bericht naar:

privacysecurityteam@boladviseurs.nl

Verwerking van persoonsgegevens

Bol Adviseurs is een full scope dienstverlener, maar ook een accountantsorganisatie. Dit brengt met zich mee dat wij bij de uitvoering van onze dienstverlening moeten voldoen aan specifieke wet- en regelgeving en beroepsvoorschriften. Bol Adviseurs is derhalve voor de verwerking van persoonsgegevens verwerkingsverantwoordelijke.

Dit betekent dat wij, in tegenstelling tot een verwerker, verantwoordelijk zijn voor de naleving van alle bepalingen uit de AVG, waaronder de beginselen van verwerking:

- Rechtmatig, behoorlijk en transparant;
- Doelbinding;
- Minimale gegevensverwerking;
- Juistheid;
- Opslagbeperking;
- Integriteit en vertrouwelijkheid.

De rechten en verplichtingen van Bol Adviseurs en de klant zijn vastgelegd in de Algemene Voorwaarden. Dit maakt het sluiten van een verwerkersovereenkomst overbodig. De Algemene Voorwaarden zijn op de website te raadplegen via de volgende link:

<https://www.boladviseurs.nl/algemene-voorwaarden/>

Informatiebeveiliging

Bol Adviseurs beschikt sinds 2018 over een Information Security Management System (ISMS). Het ISMS bevat wereldwijd geaccepteerde organisatorische en technische maatregelen op het gebied van informatiebeveiliging. Enkele voorbeelden hiervan zijn:

Leveranciers

Voor IT-gerelateerde diensten werkt Bol Adviseurs alleen samen met leveranciers die beschikken over een ISO27001-certificaat. Hierbij nemen wij kennis van de scope en de toepasselijkheid van het ISO27001-certificaat.

Medewerkers

Medewerkers van Bol Adviseurs dienen zich te houden aan gedragsregels. Dit betreffen gedragsregels op het gebied van:

- Meldplicht beveiligingsincidenten en datalekken
- Behandel informatie met zorg
- Omgang met mobiele apparatuur
- Fysieke beveiliging
- Wachtwoordbeleid
- Gebruik alleen geautoriseerde middelen

Medewerkers van Bol Adviseurs volgen een continue awareness-programma.

Externe onderzoeken

Jaarlijks wordt de kwetsbaarheid van de technische infrastructuur door een externe partij onderzocht. Het ISMS is door externe auditors van DEKRA getoetst. Op basis hiervan is een ISO27001-certificaat uitgereikt. Het certificaat is geldig van 24 september 2018 tot 24 september 2021. Binnen deze periode voeren externe auditors van DEKRA jaarlijks een audit uit.

Een kopie van het ISO27001-certificaat is opgenomen in de bijlage. De Statement of Applicability (verklaring van toepasselijkheid) wordt op verzoek toegezonden. Neem hiervoor contact op met PST via privacysecurityteam@boladviseurs.nl.



Bol Adviseurs mailt veilig

Bij Bol Adviseurs doen we er alles aan om data optimaal te beschermen en privacy te waarborgen. Daarom maken we naast regulier e-mailverkeer gebruik van tools voor een veilige communicatie. Hiermee kunnen we vertrouwelijke informatie, zoals persoonsgegevens, jaarrekeningen of backup-bestanden, veilig verzenden en ontvangen.

Voorwaarden veilig omgaan met informatie

Voorwaarden met betrekking tot technische en organisatorische maatregelen, geheimhouding, aansprakelijkheid en elektronische communicatie zijn opgenomen in de Algemene Voorwaarden. De Algemene Voorwaarden worden als bijlage toegevoegd aan de opdrachtbevestiging en zijn van toepassing op alle werkzaamheden.

De volgende artikelen van de Algemene Voorwaarden zijn specifiek van toepassing op veilig omgaan met informatie:

Artikel D

Gegevens Opdrachtgever

1. Partijen zullen in overeenstemming met de geldende privacyregelgeving technische en organisatorische maatregelen treffen en zo nodig aanpassen om een op het risico afgestemde beveiliging van de persoonsgegevens te waarborgen. Daarbij zullen partijen rekening houden met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de risico's voor de persoonsgegevens en de betrokkenen.

Artikel F

Geheimhouding en exclusiviteit

1. Opdrachtnemer is verplicht tot geheimhouding tegenover derden, die niet bij de uitvoering van de Overeenkomst zijn betrokken. Deze geheimhouding betreft alle informatie van vertrouwelijke aard die hem door Opdrachtgever ter beschikking is gesteld, waaronder begrepen alle persoonsgegevens, en de door verwerking daarvan verkregen resultaten. Deze geheimhouding geldt niet voor zover wettelijke of beroepsregels, waaronder begrepen maar niet beperkt tot de meldingsplicht voortvloeiend uit de Wet ter voorkoming van witwassen en financieren van terrorisme en andere nationale of internationale regelgeving met een vergelijkbare strekking, Opdrachtnemer een informatieplicht opleggen, of voor zover Opdrachtgever Opdrachtnemer van de geheimhoudingsplicht heeft ontheven. Deze bepaling verhindert ook niet vertrouwelijk collegiaal overleg binnen de organisatie van Opdrachtnemer, althans met de door Opdrachtnemer ingeschakelde derden, voor zover Opdrachtnemer zulks voor een zorgvuldige uitvoering van de Overeenkomst of ter zorgvuldige voldoening aan wettelijke of beroepsverplichtingen noodzakelijk acht.

2. Opdrachtnemer is gerechtigd de na bewerking verkregen cijfermatige uitkomsten, mits die uitkomsten niet te herleiden zijn tot individuele Opdrachtgevers, aan te wenden voor statistische of vergelijkende doeleinden.

3. Opdrachtnemer is niet gerechtigd de informatie die hem door Opdrachtgever ter beschikking wordt gesteld aan te wenden voor een ander doel dan waarvoor zij werd verkregen, uitgezonderd het bepaalde in lid 2, en in geval Opdrachtnemer voor zichzelf optreedt in een tucht-, civiele, bestuursrechtelijke of strafprocedure, waarbij deze stukken van belang kunnen zijn. Indien Opdrachtnemer verweten wordt een overtreding of misdrijf te hebben begaan of daaraan te hebben deelgenomen, is hij gerechtigd om Bescheiden van Opdrachtgever te openbaren aan de inspecteur der belastingen of aan de rechter, indien openbaarmaking noodzakelijk is in het kader van het voeren van verweer door Opdrachtnemer.

Artikel L

Aansprakelijkheid en vrijwaring

1. Opdrachtnemer is jegens Opdrachtgever uitsluitend aansprakelijk voor schade die het rechtstreekse gevolg is van een (samenhangende serie van) toerekenbare tekortkoming(en) in de uitvoering van de Overeenkomst. Deze aansprakelijkheid is beperkt tot het bedrag dat volgens de aansprakelijkheidsverzekeraar van Opdrachtnemer voor het betreffende geval wordt uitgekeerd, vermeerderd met het eventueel door Opdrachtnemer uit hoofde van de verzekering te dragen eigen risico. Indien, om welke reden dan ook, de aansprakelijkheidsverzekeraar niet tot uitkering overgaat, is de aansprakelijkheid van Opdrachtnemer beperkt tot het bedrag van het voor de uitvoering van de Overeenkomst in rekening gebrachte honorarium. Indien de Overeenkomst een duurovereenkomst betreft met een looptijd van meer dan één jaar, wordt het hiervoor bedoelde bedrag gesteld op drie maal het bedrag van het honorarium dat in de twaalf maanden voorafgaand aan het ontstaan van de schade in rekening is gebracht aan Opdrachtgever. In geen geval zal de totale vergoeding van de schade op grond van dit artikel meer bedragen dan € 300.000 per gebeurtenis, waarbij een reeks samenhangende gebeurtenissen geldt als één gebeurtenis, tenzij partijen - gezien de omvang van de Opdracht of de risico's die met de Opdracht gepaard gaan - reden zien om bij het aangaan van de Overeenkomst af te wijken van dit maximum.

Artikel Q

Elektronische communicatie en elektronisch deponeren van jaarstukken

1. Opdrachtnemer maakt gebruik van elektronische communicatiemiddelen. Opdrachtgever stemt in met het gebruik door Opdrachtnemer van een elektronische handtekening als bedoeld in artikel 3:15a Burgerlijk Wetboek. Tijdens de uitvoering van de Opdracht kunnen Opdrachtgever en Opdrachtnemer door middel van elektronische middelen met elkaar communiceren en/of gebruik maken van elektronische opslag (zoals cloud-toepassingen). Behoudens voor zover schriftelijk anders is overeengekomen, mogen partijen ervan uitgaan dat verzending van correct geadresseerde faxberichten, e-mails (met inbegrip van e-mails die via internet worden verstuurd) en voicemailberichten ongeacht of deze vertrouwelijke informatie of stukken bevatten die op de Opdracht betrekking hebben, over en weer worden aanvaard. Hetzelfde geldt voor andere door de andere partij gebruikte of aanvaarde communicatiemiddelen.

2. Opdrachtgever en Opdrachtnemer zijn jegens elkaar niet aansprakelijk voor schade die eventueel voortvloeit bij één of ieder van hen ten gevolge van het gebruik van elektronische middelen van communicatie, netwerken, applicaties, elektronische opslag, of overige systemen waaronder – maar niet beperkt tot – schade ten gevolge van niet-aflevering of vertraging bij de aflevering van elektronische communicatie, omissies, vervorming, onderschepping of manipulatie van elektronische communicatie door derden of door programmatuur/apparatuur gebruikt voor verzending, ontvangst of verwerking van elektronische communicatie, overbrenging van virussen en



het niet of niet goed functioneren van het telecommunicatienetwerk of andere voor elektronische communicatie benodigde middelen, behoudens voor zover de schade het gevolg is van opzet of grove schuld. Het voorgaande geldt eveneens voor het gebruik dat Opdrachtnemer daarvan maakt in haar contacten met derden.

4. Zowel Opdrachtgever als Opdrachtnemer zullen al hetgeen redelijkerwijs van ieder van hen verwacht mag worden doen of nalaten ter voorkoming van het optreden van voornoemde risico's.

Vragen?

Heb je naar aanleiding van dit infodoc nog vragen, neem dan gerust contact op met het PST via privacysecurityteam@boladviseurs.nl

Bijlage 1: Certificaat ISO 27001



CERTIFICAAT

Nummer: 2219822

Het managementsysteem van de op het addendum vermelde organisatie(s) en/of locaties van:

Bol Accountants B.V.
h.o.d.n. Bol Adviseurs en Bol International
 Spoorstraat 73
 5831 CK Boxmeer

en de toepassing daarvan voldoet aan de voorwaarden gesteld in:

ISO/IEC 27001:2013

Voor het toepassingsgebied:

Klanten ondersteunen bij alle facetten van het ondernemerschap en de beheerorganisatie en de IT die hiervoor nodig is, met diensten:

- voor bedrijven,
- voor werkgevers en personeel,
- tussen zakelijk en privé,
- voor ondernemers, en
- voor internationaal ondernemen

De selectie van risico reducerende maatregelen is beschreven in de verklaring van toepasselijkheid; Versie 4 mei 2018.

Dit certificaat is geldig tot: 24 september 2021
 Dit certificaat is geldig vanaf: 24 september 2018
 Gecertificeerd sinds: 24 september 2018

Dit certificaat is geldig voor de organisatie(s) en/of locaties genoemd op het addendum.

DEKRA Certification B.V.

drs. G.J. Zoetbrood
 Directeur

R.C. Verhagen
 Certificatie Manager

© Integrale publicatie van dit certificaat alsmede de bijbehorende rapporten is uitsluitend in hun geheel toegestaan.



DEKRA Certification B.V. Meander 1051, 6825 MJ Arnhem Postbus 5185, 6802 ED Arnhem, Nederland
 T +31 88 96 83000 F +31 88 96 83100 www.dekra-certification.nl Handelsregister 09085396

ADDENDUM

Behorende bij certificaat van: 2219822

Het managementsysteem van de organisatie(s) en/of locaties van:

Bol Accountants B.V. h.o.d.n. Bol Adviseurs en Bol International

Spoorstraat 73
5831 CK Boxmeer

Gecertificeerde vestiging(en):

Bol Accountants B.V.
Eisenhowerweg 14 A
5466 AC Veghel

Bol Accountants B.V.
Bijsterhuizen 3165
6546 AS Wijchen

Bol Accountants B.V.
Hoogakker 15
5802 MA Venray

Bol Accountants B.V. h.o.d.n.
Bol Adviseurs en Bol International
Spoorstraat 73
5831 CK Boxmeer

Dit addendum is geldig tot: 24 september 2021
Dit addendum is geldig vanaf: 24 september 2018