REGLEMENT VERWERKING PERSOONSGEGEVENS

Artikel 1 Definities

1.1 In dit reglement wordt verstaan onder:

(a) AVG: Verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene verordening gegevensbescherming), publicatieblad nr. L119 van 4 mei 2016, p.1 e.v.;
(b) BDO: BDO Holding B.V. en elk van de met haar in een groep verbonden rechtspersonen, die ieder afzonderlijk onder de merknaam 'BDO' actief zijn op een bepaald terrein van de zakelijke dienstverlening (accountancy, belastingadvies en consultancy);
(c) Klant: degene die aan BDO opdracht heeft gegeven tot het verrichten van werkzaamheden;
(d) Betrokkene: de natuurlijke persoon die aan de hand van persoonsgegevens geïdentificeerd of identificeerbaar is.
(e) Leverancier: degene die aan BDO diensten verleent of goederen levert;
(f) Medewerker: degene die op basis van een arbeids- of andersoortige overeenkomst werkzaamheden ten behoeve van BDO verricht;
(g) UAVG: Wet van 16 mei 2018, Stb. 2018, 144, houdende regels ter uitvoering van de AVG (Uitvoeringswet Algemene verordening gegevensbescherming).

1.2 Overigens geldt dat alle in dit reglement opgenomen begrippen, die gelijkluidend zijn aan de in artikel 4 van de AVG gedefinieerde begrippen, de zelfde betekenis hebben als in dat artikel bepaald.

Artikel 2 Toepasselijkheid

2.1 Dit reglement is van toepassing op de verwerking van persoonsgegevens door BDO als verwerkingsverantwoordelijke.

2.2 Dit reglement is niet van toepassing op de verwerking van persoonsgegevens door BDO als verwerker. In dat geval wordt de verhouding tussen BDO en de desbetreffende verwerkingsverantwoordelijke beheerst door een verwerkingsovereenkomst in de zin van artikel 28 lid 3 van de AVG.

2.3 Dit reglement heeft tevens de betekenis van het in artikel 30 lid 1 van de AVG bedoelde register van verwerkingsactiviteiten.

Artikel 3 Verwerkingsverantwoordelijke

3.1 Als verwerkingsverantwoordelijke onder dit reglement geldt BDO Holding B.V., statutair gevestigd te Eindhoven, ongeacht of de verwerking van persoonsgegevens door BDO Holding B.V. of door een groepsmaatschappij van BDO Holding B.V. geschiedt.

3.2 BDO Holding B.V. heeft als verwerkingsverantwoordelijke een functionaris voor gegevensbescherming voor BDO als geheel aangewezen met de titel 'Data Protection Officer'.

3.3 Betrokkenen kunnen zich voor de uitoefening van hun rechten in het kader van dit reglement en voor alle overige aangelegenheden die verband houden met de verwerking van persoonsgegevens door BDO, ongeacht of die verwerking door BDO Holding B.V. of

door een groepsmaatschappij van BDO Holding B.V. geschiedt, tot de in artikel 3.2 bedoelde functionaris wenden. De contactgegevens van die functionaris zijn:

BDO Holding B.V.
T.a.v. Data Protection Officer
Postbus 182
5600 AD Eindhoven
e-mail: privacy@bdo.nl

Artikel 4 Doel verwerking van persoonsgegevens

4.1 BDO verwerkt persoonsgegevens voor de navolgende doelen:

(a) de uitvoering van overeenkomsten met Klanten;
(b) de uitvoering van overeenkomsten met Leveranciers;
(c) de uitvoering van overeenkomsten met Medewerkers;
(d) de uitoefening van uit overeenkomsten voortvloeiende (vorderings)rechten;
(e) het verrichten van marketingactiviteiten;
(f) het verrichten van wervingsactiviteiten;
(g) de voldoening aan op BDO rustende wettelijke verplichtingen;
(h) het (specifieke) doel waarvoor persoonsgegevens met toestemming van Betrokkene worden verwerkt.

4.2 De verwerking van persoonsgegevens door BDO geschiedt op basis van de navolgende rechtsgronden:

- wat betreft de in artikel 4.1 onder (a) tot en met (d) genoemde doelen: artikel 6 lid 1 onder b) van de AVG (uitvoering overeenkomst);
- wat betreft het in artikel 4.1 onder (e) genoemde doel: artikel 6 lid 1 onder a) van de AVG (toestemming Betrokkene) of artikel 6 lid 1 onder f) van de AVG (behartiging gerechtvaardigd belang BDO);
- wat betreft het in artikel 4.1 onder (f) genoemde doel: artikel 6 lid 1 onder a) van de AVG (toestemming Betrokkene);
- wat betreft het in artikel 4.1 onder (g) genoemde doel: artikel 6 lid 1 onder c) van de AVG (voldoen aan wettelijke verplichtingen);
- wat betreft het in artikel 4.1 onder (h) genoemde doel: artikel 6 lid 1 onder a) van de AVG (toestemming Betrokkene).

4.3 Indien de verwerking van persoonsgegevens door BDO berust op toestemming van de Betrokkene, heeft Betrokkene te allen tijde het recht de toestemming in te trekken. De intrekking van de toestemming geldt alleen voor de toekomst.

Artikel 5 Categorieën van Betrokkenen en van persoonsgegevens

5.1 BDO verwerkt persoonsgegevens van de navolgende categorieën van Betrokkenen, voor zover zij natuurlijke personen zijn:

(a) Klanten;
(b) Leveranciers;
(c) Medewerkers;
(d) Personen die toestemming hebben gegeven voor de verwerking van persoonsgegevens met het oog op het verrichten van marketingactiviteiten of van wervingsactiviteiten;
(e) Personen die toestemming hebben gegeven voor de verwerking van persoonsgegevens met het oog op een ander (specifiek) doel.

5.2 BDO verwerkt de navolgende categorieën van persoonsgegevens, doch uitsluitend voor zover de verwerking daarvan noodzakelijk is voor het desbetreffende doel:

Identificatiegegevens

(a) naam;
(b) adres;
(c) geboortedatum;
(d) geboorteplaats;
(e) burgerservicenummer;
(f) identiteitsbewijsnummer;
(g) telefoonnummer;
(h) e-mailadres;
(i) IP-adres;

Transactiegegevens

(j) bankrekeningnummer;
(k) bijschrijvingen op, afschrijvingen van en overboekingen naar bankrekeningen;

Financiële gegevens

(l) belastingaangiften;
(m) financiële- en adviesrapportages;
(n) facturen;
(o) creditnota's;
(p) loonstroken;
(q) betaalgedrag;
(r) inkomen;

Audiovisuele gegevens

(s) bewakingsbeelden gemaakt bij BDO-kantoren.

Artikel 6 Verstrekking persoonsgegevens aan derden

6.1 BDO verstrekt persoonsgegevens aan de navolgende ontvangers, doch uitsluitend voor zover de verstrekking daarvan noodzakelijk is voor het desbetreffende doel of BDO daartoe krachtens de wet gehouden is:

(a) Belastingdienst;
(b) Kamer van Koophandel via Digipoort;
(c) Opsporingsinstanties;
(d) Toezichthoudende autoriteiten.

6.2 BDO zal Betrokkene informeren omtrent een verstrekking van persoonsgegevens aan de in artikel 6.1 genoemde categorieën van ontvangers, tenzij haar dit krachtens de wet verboden is.

Artikel 7 Verwerking of doorgifte persoonsgegevens in of aan derde landen

7.1 BDO verwerkt persoonsgegevens niet in en geeft Persoonsgegevens niet door aan een land buiten de Europese Unie of de Europese Economische Ruimte, waarvan niet bij besluit van de Europese Commissie is vastgesteld dat het een passend beschermingsniveau in de zin van artikel 45 lid 1 van de AVG waarborgt, tenzij:

(a) Betrokkene daarvoor uitdrukkelijk en schriftelijk toestemming heeft verleend, of
(b) passende waarborgen in de zin van artikel 46 lid 1 van de AVG bestaan.

7.2 BDO zal Betrokkene informeren omtrent het voornemen persoonsgegevens in een derde land te verwerken of aan een derde land door te geven met vermelding van de in artikel 13 lid 1 onder e) van de AVG bedoelde gegevens.

Artikel 8 Bewaring van persoonsgegevens

8.1 BDO bewaart persoonsgegevens niet langer dan voor het doel waarvoor de persoonsgegevens worden verwerkt noodzakelijk is en voorts met inachtneming van de ter zake geldende wettelijke bewaartermijnen. Daarna worden persoonsgegevens geanonimiseerd, gepseudonimiseerd of gewist.

8.2 BDO kan persoonsgegevens langer bewaren dan in artikel 8.1 is bepaald, doch uitsluitend voor zover die persoonsgegevens voor historisch of wetenschappelijk onderzoek of voor statistische doeleinden worden bewaard en worden verwerkt met inachtneming van het bepaalde in artikel 89 lid 1 van de AVG.

Artikel 9 Beveiliging van persoonsgegevens

9.1 BDO treft passende technische en organisatorische maatregelen om de persoonsgegevens te beveiligen tegen verlies en tegen enige vorm van onbevoegde of onrechtmatige verwerking daarvan, daaronder begrepen onnodige verzameling en verdere verwerking daarvan, daarbij rekening houdend met hetgeen in artikel 32 leden 1 en 2 van de AVG wordt genoemd. Een algemene beschrijving van de hiervoor bedoelde maatregelen is in Bijlage A opgenomen.

9.2 BDO treft maatregelen om ervoor te zorgen dat persoonsgegevens uitsluitend worden verwerkt door Medewerkers die daartoe uit hoofde van hun functie of taak bevoegd zijn en dat door Medewerkers niet meer persoonsgegevens worden verwerkt dan voor het desbetreffende doel noodzakelijk is.

Artikel 10 Verwerkers

10.1 BDO is bevoegd derden als verwerkers bij de verwerking van persoonsgegevens in te schakelen. De verwerkers die door BDO voor de verwerking van de Persoonsgegevens zijn ingeschakeld staan vermeld op Bijlage B.

10.2 De rechtsverhouding tussen BDO en de in artikel 10.1 bedoelde verwerkers wordt beheerst door een tussen BDO en elk van die verwerkers gesloten verwerkingsovereenkomst in de zin van artikel 28 lid 3 van de AVG.

Artikel 11 Rechten van Betrokkene

11.1 Betrokkene heeft recht op:

(a) inzage van hem betreffende persoonsgegevens die door BDO worden verwerkt en van informatie als bedoeld in artikel 15 lid 1 van de AVG;
(b) rectificatie of vervollediging van hem betreffende onjuiste of onvolledige persoonsgegevens die door BDO worden verwerkt conform artikel 16 van de AVG;
(c) wissing van hem betreffende persoonsgegevens die door BDO worden verwerkt in de gevallen genoemd in artikel 17 lid 1 van de AVG;
(d) beperking van de verwerking van hem betreffende persoonsgegevens door BDO in de gevallen genoemd in artikel 18 lid 1 van de AVG;
(e) verkrijging van hem betreffende persoonsgegevens in een gestructureerde, gangbare en machineleesbare vorm en overdracht van die persoonsgegevens aan

een andere verwerkingsverantwoordelijke, in de gevallen genoemd in artikel 20 lid 1 van de AVG.

11.2 Betrokkene heeft voorts het recht bezwaar te maken tegen de verwerking van hem betreffende persoonsgegevens en staking daarvan te verzoeken in de gevallen genoemd in artikel 21 leden 1 en 2 van de AVG.

11.3 De uitoefening van de in de artikelen 11.1 en 11.2 genoemde rechten geschiedt door indiening van een daartoe strekkend verzoek (hierna: het 'verzoek') door of namens Betrokkene bij BDO. Het verzoek wordt gestuurd aan het in artikel 3.3 genoemde adres.

11.4 Het verzoek dient gegevens te bevatten die het mogelijk maken Betrokkene te identificeren. Bij gebreke van dergelijke gegevens kan BDO verlangen dat Betrokkene zich identificeert. Die identificatie kan plaatsvinden op een van de kantoren van BDO. Het verzoek wordt geacht te zijn ontvangen, zodra de identiteit van Betrokkene vast staat.

11.5 BDO neemt het verzoek zo spoedig mogelijk na ontvangst in behandeling en deelt Betrokkene binnen één maand nadien mede op welke wijze gevolg aan het verzoek is gegeven. Die termijn kan met twee maanden worden verlengd. Ingeval van verlenging, zal Betrokkene daarvan binnen één maand na ontvangst van het verzoek in kennis worden gesteld.

11.6 Indien geen gevolg aan het verzoek wordt gegeven, deelt BDO dit binnen een maand na ontvangst van het verzoek onder opgaaf van redenen aan Betrokkene mede. In dat geval heeft Betrokkene de mogelijkheid een klacht bij de Autoriteit Persoonsgegevens in te dienen of een verzoekschrift als bedoeld in artikel 35 UAVG bij de rechtbank in te dienen.

11.7 De indiening en behandeling van het verzoek, de verstrekking van informatie naar aanleiding van het verzoek en het treffen van maatregelen ter uitvoering van het verzoek zijn kosteloos.

11.8 Indien een verzoek kennelijk ongegrond of buitensporig is, bijvoorbeeld omdat het herhaaldelijk wordt gedaan, is BDO bevoegd hetzij administratieve kosten in rekening te brengen hetzij geen gevolg aan het verzoek te geven.

Artikel 12 Geschilbeslechting

12.1 Indien Betrokkene het niet eens is met de beslissing van BDO geen gevolg aan het in artikel 11.3 bedoelde verzoek te geven of indien tussen Betrokkene en BDO anderszins geschil over de toepassing van dit reglement bestaat, heeft Betrokkene op grond van artikel 36 UAVG de mogelijkheid zich tot de Autoriteit Persoonsgegevens te wenden met het verzoek te bemiddelen.

12.2 Indien Betrokkene van de in artikel 12.1 bedoelde mogelijkheid gebruik maakt, zal BDO alle medewerking aan een behandeling van het geschil door de Autoriteit Persoonsgegevens verlenen.

Artikel 13 Kennisgevingen en mededelingen

13.1 Alle kennisgevingen of mededelingen van BDO aan Betrokkene in het kader van dit reglement geschieden schriftelijk en worden gericht aan het (e-mail)adres van de Betrokkene zoals dat is opgenomen in de administratie van BDO, tenzij daartoe door Betrokkene uitdrukkelijk en schriftelijk een ander adres is opgegeven.

13.2 Indien Betrokkene daarom verzoekt, kunnen de in artikel 13.1 bedoelde kennisgevingen of mededelingen ook mondeling door BDO aan Betrokkene worden gedaan, mits de identiteit van Betrokkene vast staat.

Artikel 14 Slotbepaling

14.1 Dit reglement is vastgesteld door het bestuur van BDO Holding B.V. en geldt met ingang van 1 januari 2019 voor BDO als geheel.

14.2 Dit reglement kan te allen tijde bij daartoe strekkend besluit van het bestuur van BDO Holding B.V. worden gewijzigd. De wijziging van het reglement wordt schriftelijk vastgelegd en wordt bekend gemaakt op de wijze als bij het besluit tot wijziging te bepalen.

Bijlage A Algemene beschrijving beveiligingsmaatregelen.

BDO ICT voldoet voor de beveiliging van haar organisatie en infrastructuur aan de internationaal erkende standaard voor informatiebeveiliging: de norm ISO 27001. De norm is van toepassing op de ICT-processen: informatie, informatiesystemen, netwerken, en op het IT-personeel dat de bedrijfsprocessen ondersteunt.

Door het regelmatig uitvoeren van informatiebeveiligingscontroles en van in- en externe audits blijft het informatiebeveiligingsniveau van BDO hoog. BDO heeft alle beheersmaatregelen geselecteerd vanuit risicoanalyses en uit de baselines/beleid. Alle maatregelen uit de norm ISO 27001 zijn geïmplementeerd en de audits zijn uitgevoerd door BDO IT audit en BSI.

Het afschrift het ISO 27001 certificaat en bijbehorende verklaring van toepasselijkheid kunnen worden opgevraagd bij de afdeling Quality & Riskmanagement via eerdergenoemd e-mailadres.

De basis voor deze certificering ligt in het informatiebeveiligings- en privacybeleid van BDO. Dit beleid zorgt ervoor dat de organisatie van BDO blijft voldoen aan de norm ISO 27001. Verantwoordelijk hiervoor is de afdeling Quality & Riskmanagement. Een team van Information Security & Privacy Officers is verantwoordelijk voor het rapporteren over beveiligingsincidenten en relevante ontwikkelingen op het gebied van informatiebeveiliging en privacy aan het multidisciplinair samengestelde Forum Informatiebeveiliging binnen BDO.

Binnen het informatiebeveiligingsbeleid van BDO zijn verschillende beheersmaatregelen actief die zijn onderverdeeld in onderstaande categorieën:

- Beveiliging van de fysieke ICT-omgeving;
- Ontwikkeling en onderhoud van informatiesystemen;
- Beheer van bedrijfsmiddelen;
- Medewerkers;
- Beveiligde applicaties en toepassingen;
- Leveranciersrelaties;
- Beheer van informatiebeveiligingsincidenten.

Bijlage B Lijst van verwerkers

- AFAS
- Basecone
- BDO International
- Carerix
- CTAC
- KPN
- Loket
- Microsoft
- PKIsigning
- Proquro
- Reed Business Information
- RobotX
- Smartbooqing
- Thomson Reuters
- Twinfield