Algemene Voorwaarden

Versie 1.3 van 16.8.2018

Artikel 1. Toepasselijkheid en totstandkoming van overeenkomst

1.1. Deze algemene voorwaarden zijn van toepassing op alle overeenkomsten, rechtsbetrekkingen en offertes met of van de besloten vennootschap met beperkte aansprakelijkheid SafeHarbour Solutions B.V. gevestigd te Rotterdam, en aan haar gelieerde ondernemingen, zoals dochter-, moeder- of zusterondernemingen, die zich bedienen van deze voorwaarden, hierna te noemen "SafeHarbour"

1.2. De toepasselijkheid van algemene dan wel specifieke (inkoop)voorwaarden van opdrachtgever wordt hierbij uitdrukkelijk door SafeHarbour van de hand gewezen, en zijn derhalve niet van toepassing.

1.3. Alle door SafeHarbour gedane offertes en/of aanbiedingen zijn vrijblijvend, tenzij daaruit anders blijkt. Als er een termijn genoemd wordt in de offerte/aanbieding betreft de termijn alleen de geldigheid van de offerte/aanbieding en tast het niet de vrijblijvendheid aan.

1.4. Tenzij uitdrukkelijk anders is overeengekomen komt de overeenkomst tussen SafeHarbour en opdrachtgever tot stand door integrale aanvaarding van de offerte door opdrachtgever. Aanvaarding vindt plaats door het ondertekenen van de opdrachtbevestiging door opdrachtgever. De overeenkomst kan ook tot stand komen door het ondertekenen door beide partijen van een (mantel)contract waarin onderhavige algemene voorwaarden van toepassing verklaard worden.

1.5. Bij een afwijkende aanvaarding van een offerte houdt SafeHarbour zich het recht voor een nieuwe offerte uit te brengen welke in de plaats treedt van de vorige offerte, in die zin dat de oude offerte –indien en voor zover dat al niet het geval was- haar geldigheid verliest. De nieuwe offerte kan door opdrachtgever worden aanvaard op eenzelfde wijze als hiervoor vermeld.

1.6. Het feitelijk beginnen met uitvoeren van de overeenkomst aan de zijde van de opdrachtgever, daaronder mede begrepen, doch niet uitsluitend, het betalen van facturen zoals gestuurd door SafeHarbour, geldt als aanvaarding van onderhavige voorwaarden.

Artikel 2. Uitvoering van de overeenkomst

2.1. De overeenkomst wordt door SafeHarbour vakkundig en integer uitgevoerd. Indien eventuele gedragsregels (*code of conduct*) onderdeel uitmaken van de overeenkomst zal SafeHarbour zich tot een uiterste inspannen zich daaraan te houden. Indien en voor zover de uitvoering op gespannen voet komt te staan met die eventuele gedragsregels zal SafeHarbour met opdrachtgever onverwijld in overleg treden teneinde dit voor opdrachtgever zo goed mogelijk –in het licht van de gedragsregels- op te lossen.

2.2. Opdrachtgever verbindt zich jegens SafeHarbour om de leveringen in overeenstemming met de overeenkomst te aanvaarden en de voorziene medewerking te verlenen.

2.3. In verband met de continuïteit van de werkzaamheden in het kader van de uitvoering van de overeenkomst zal opdrachtgever een contactpersoon of contactpersonen aanwijzen die voor de duur van de werkzaamheden van SafeHarbour als zodanig zal/zullen fungeren. Contactpersonen van opdrachtgever zullen beschikken over de nodige ervaring, specifieke materiekennis en inzicht in de gewenste doelstellingen van opdrachtgever. Indien deze persoon niet de kwalificaties heeft welke redelijkerwijs gezien de aard van de opdracht verwacht mag worden, houdt SafeHarbour zich het recht voor de uitvoering van de overeenkomst op te schorten, zonder gehouden zijn tot enige schadevergoeding, tot dat opdrachtgever deze persoon heeft vervangen door een persoon met de juiste kwalificaties.

2.4. Opdrachtgever dient SafeHarbour tijdig en kosteloos te voorzien van alle informatie en gegevens die nodig zijn voor de uitvoering van de overeenkomst, waaronder in elk geval begrepen technische gegevens, applicaties, bestanden, documentatie, testgegevens, werkbeschrijvingen, beschrijvingen van bedrijfsprocessen, beschrijvingen van (informatie)beveiliging, en/of overige relevante informatie. Opdrachtgever staat in voor, en garandeert de juistheid van die hiervoor bedoelde gegevens. Opdrachtgever is voorts verantwoordelijk voor, en aanvaardt het risico van, mogelijke problemen en/of aanspraken voortvloeiende uit de inhoud, nauwkeurigheid, volledigheid en consistentie van al dergelijke door opdrachtgever verstrekte gegevens, materialen en informatie.

2.5. Indien voor de uitvoering van de overeenkomst noodzakelijke informatie niet, niet-tijdig of niet overeenkomstig de afspraken ter beschikking wordt gesteld aan SafeHarbour of indien opdrachtgever en/of haar leveranciers op andere wijze niet aan haar verplichtingen voldoet respectievelijk voldoen, daaronder mede begrepen maar niet uitsluitend het niet afdoende meewerken en/of inzetten, heeft SafeHarbour het recht de nakoming van haar verplichtingen op te schorten zonder dat zij tot enige schadevergoeding gehouden kan worden. SafeHarbour is voorts gerechtigd om de in dit verband extra gemaakte kosten in rekening te brengen bij opdrachtgever.

2.6. Alle door SafeHarbour opgegeven, of op enig moment op te geven, leveringstermijnen gelden altijd bij benadering en zijn nimmer te beschouwen als fatale termijnen. Derhalve kunnen de indicaties van leveringstermijnen op geen enkele wijze een toerekenbare tekortkoming van de kant van SafeHarbour tot gevolg hebben, noch is de opdrachtgever in enig geval gerechtigd aanspraak te maken op enige schadevergoeding.

2.7. Indicaties van leveringstermijnen zijn gebaseerd op de ten tijde van de overeenkomst geldende werkomstandigheden en tijdige aanlevering van materialen, documenten en/of werkinstructies. Indien vertraging ontstaat ten gevolge van wijzigingen in genoemde omstandigheden en/of ten gevolge van niet tijdige levering van materialen, documenten en/of werkinstructies van leveranciers waarvan SafeHarbour en/of opdrachtgever zich bedient, wordt de leveringstermijn voor zover nodig verlengd en/of vervalt deze. Dit zonder dat het recht van SafeHarbour vervalt zoals in lid 5 van dit artikel is uiteengezet.

2.8. Indien vertraging is te wijten aan een handelen of nalaten van opdrachtgever en/of haar leveranciers, bijvoorbeeld het onvoldoende verlenen van medewerking (daaronder mede begrepen het beantwoorden van vragen), dient opdrachtgever de eventuele leegloopuren van de werknemers van SafeHarbour te vergoeden, dit op eerste verzoek van SafeHarbour.

Artikel 3. Advisering, projectmanagement en consultancy

3.1. Onverminderd de overige bepalingen uit deze algemene voorwaarden zijn de navolgende leden zijn van toepassing als de opdracht gedeeltelijk of geheel bestaat uit advisering, consultancy en/of projectmanagement. In dit laatste geval wordt bedoeld projectmanagement dat door opdrachtgever wordt afgenomen om een (extern) project te managen, anders dan een opdracht waarbij project management aan de zijde van SafeHarbour behoort te zijn inbegrepen.

3.2. SafeHarbour zal zich naar beste kunnen inspannen de dienstverlening met zorg uit te voeren, in voorkomend geval overeenkomstig de met opdrachtgever schriftelijk vastgelegde afspraken en procedures. Alle diensten van SafeHarbour worden uitgevoerd op basis van een inspanningsverbintenis, tenzij en voor zover in de schriftelijke overeenkomst SafeHarbour uitdrukkelijk een resultaat heeft toegezegd en het betreffende resultaat tevens met voldoende bepaaldheid is omschreven.

3.3. Slechts indien dit schriftelijk is overeengekomen, is SafeHarbour gehouden bij de uitvoering van de dienstverlening tijdige en verantwoord gegeven aanwijzingen van opdrachtgever op te volgen. SafeHarbour is niet verplicht aanwijzingen op te volgen die de inhoud of omvang van de overeengekomen dienstverlening wijzigen of aanvullen.

3.4. Indien een overeenkomst tot dienstverlening is aangegaan met het oog op uitvoering door een bepaalde persoon, is SafeHarbour steeds gerechtigd na overleg met opdrachtgever deze persoon te vervangen door één of meer andere personen met dezelfde of vergelijkbare kwalificaties.

3.5. De dienstverlening van SafeHarbour wordt uitsluitend verricht op en planningen en werkzaamheden zijn erop gebaseerd dat, tenzij uitdrukkelijk anders overeengekomen met opdrachtgever, werkzaamheden door SafeHarbour worden verricht op de gebruikelijke werkdagen en -tijden van SafeHarbour.

3.6. Tenzij schriftelijk anders overeengekomen, is het gebruik dat opdrachtgever maakt van een door SafeHarbour afgegeven advies steeds voor rekening en risico van opdrachtgever.

3.7. SafeHarbour zal opdrachtgever op de schriftelijk overeengekomen wijze periodiek informeren over de uitvoering van de werkzaamheden via de door opdrachtgever aangewezen contactpersoon. Opdrachtgever zal SafeHarbour schriftelijk op voorhand omstandigheden melden die voor SafeHarbour van belang zijn of kunnen zijn, zoals over de wijze van rapporteren, de vraagpunten waarvoor opdrachtgever aandacht wenst, prioriteitenstelling van opdrachtgever, beschikbaarheid van middelen en personeel van opdrachtgever en bijzondere of voor SafeHarbour mogelijk niet bekende feiten of omstandigheden. Opdrachtgever zal zorgdragen voor de verdere verspreiding en kennisneming van de door SafeHarbour verstrekte inlichtingen binnen de organisatie van opdrachtgever en deze inlichtingen mede op basis daarvan beoordelen en SafeHarbour hiervan op de hoogte stellen.

3.8. Indien een door SafeHarbour ingezette medewerker deel uitmaakt van een project- of stuurgroep waarvan tevens één of meer personen deel uitmaken die door opdrachtgever zijn aangewezen, dan zal de verstrekking van inlichtingen plaatsvinden op de wijze zoals voor de project- of stuurgroep is voorgeschreven. Besluiten genomen in een dergelijk samengestelde project- of stuurgroep binden SafeHarbour slechts indien de besluitvorming geschiedt met inachtneming van hetgeen daaromtrent schriftelijk tussen partijen is overeengekomen of, bij gebreke van schriftelijke afspraken daaromtrent, indien SafeHarbour de besluiten schriftelijk heeft aanvaard. SafeHarbour is nimmer gehouden een besluit te aanvaarden indien dat naar zijn oordeel onverenigbaar is met de inhoud van de overeenkomst van partijen. Opdrachtgever staat ervoor in dat de personen die door hem zijn aangewezen om deel uit te maken van een project- of stuurgroep waaraan ook personen van SafeHarbour deel uitmaken, gerechtigd zijn voor opdrachtgever bindende besluiten te nemen.

3.9. Zonder voorafgaande schriftelijke toestemming van SafeHarbour is opdrachtgever niet gerechtigd een mededeling aan derden te doen over de werkwijze, de methoden en technieken van SafeHarbour en/of de inhoud van de adviezen of rapportages van SafeHarbour. Opdrachtgever zal de adviezen of rapportages van SafeHarbour niet aan een derde verstrekken of anderszins openbaar maken.

Artikel 4. Bepalingen inzake Software as a Service (SaaS)

4.1. Onverminderd de overige bepalingen uit deze algemene voorwaarden zijn de navolgende leden van toepassing als de opdracht gedeeltelijk of geheel bestaat uit een dienst die zich als SaaS laat definiëren, te weten: het door SafeHarbour op afstand beschikbaar stellen en houden van functionaliteit van programmatuur aan opdrachtgever via internet of een ander netwerk, zonder dat aan opdrachtgever een fysieke drager met de desbetreffende programmatuur wordt verstrekt (anders dan voor eventuele cliënt-programmatuur), zoals bijvoorbeeld online (privacy)handboeken

4.2. Opdrachtgever zal in het kader van het afnemen van de dienst handelen als een professionele gebruiker en in dat kader in ieder geval:

a. geen onoordeelkundig, ongeautoriseerd, onwettig of onoorbaar gebruik of gebruik niet overeenkomstig het gebruiksdoel maken van de dienst van SafeHarbour;
b. geen data op de servers van SafeHarbour plaatsen die in strijd zijn met de rechten, waaronder de intellectuele eigendomsrechten, van SafeHarbour of derden;
c. een inbreuk maken op intellectuele eigendomsrechten van SafeHarbour of derden;
d. geen virussen verspreiden;
e. geen ongevraagde e-mail of berichten verspreiden (spam);

f. derden niet toestaan gebruik te maken van de dienst zonder voorafgaande uitdrukkelijke schriftelijke toestemming van SafeHarbour;
g. de dienst, inclusief programmatuur, niet nader inrichten c.q. parametriseren zodanig dat de systeembelasting substantieel groter wordt of de stabiliteit van de functionaliteit lager wordt;
h. geen verstoring van het functioneren van ICT-infrastructuur van SafeHarbour, infrastructuur van derden en/of koppelingen tussen infrastructuren door (de inhoud of intensiteit van) het dataverkeer of door het handelen en/of nalaten van opdrachtgever veroorzaken.

4.3. De dienstverlening inzake SaaS wordt geleverd conform de tussen partijen afgesproken Service Level Agreement (SLA). Bij gebreke waarvan wordt de dienst zodanig geleverd dat SafeHarbour zich zal inspannen, zonder dat daar rechten aan ontleend kunnen worden, dat de dienst welke onderdeel uitmaakt van de overeenkomst ten minste 95% (vijfennegentig procent) beschikbaar is per kalenderjaar.

4.4. SafeHarbour zal ernaar streven dat aan alle uit te voeren activiteiten met betrekking tot een door opdrachtgever gedaan beroep op support, daaronder mede begrepen behandelen van vragen van gebruikers en het oplossen van gebreken, zonder onnodige vertraging zullen worden begonnen en zo mogelijk voltooid.

4.5. Het in behandeling nemen van een gebrek gebeurt alleen indien en voor zover dit gebrek aantoonbaar dan wel reproduceerbaar is. Onder gebrek wordt verstaan het niet, dan wel niet volledig, voldoen van functionaliteit aan de overeengekomen specificaties.

4.6. Indien en voor zover de tijd die het oplossen van een gebrek in beslag neemt, of wordt vermoed in beslag zal nemen, van dusdanige duur is, dat vermoed wordt dat de beschikbaarheid van de functionaliteit zal worden aangetast, zal SafeHarbour trachten te voorzien in een tijdelijke, toereikende oplossing.

4.7. Gebreken in beschikbaarheid welke zijn veroorzaakt door:
a. onoordeelkundig gebruik door gebruiker;
b. het werken met apparatuur en/of (browser)programmatuur welke niet voldoen aan de vooraf door SafeHarbour goedgekeurde specificaties;

vallen nimmer binnen de reikwijdte van de overeenkomst. Alleen op grond van een schriftelijke bevestiging van opdrachtgever zal SafeHarbour zo mogelijk bedoelde gebreken herstellen, zulks tegen haar alsdan geldende tarieven.

4.8. SafeHarbour kan, in het geval dat gebruikers niet over adequate kennis van de functionaliteit en/of de SaaS-dienst beschikken, van opdrachtgever eisen dat deze opleidingen van SafeHarbour betrekt ten einde de kennis van de gebruikers op een dusdanig niveau te brengen dat zij niet langer een onevenredig beroep op support doen, dan wel gebruikers anderszins benodigde kennis zullen opdoen. SafeHarbour zal de redelijkheid van deze eis inschatten op basis van haar (support)historie. Indien opdrachtgever hieraan geen gehoor geeft heeft SafeHarbour het recht haar verplichtingen in het kader van support op te schorten totdat de kennis van gebruikers op voldoende niveau is gebracht, zonder dat Afnemer recht heeft op restitutie van reeds betaalde gelden of enige schadevergoeding.

4.9. SafeHarbour bepaalt zelfstandig en zonder raadpleging van opdrachtgever het versiebeleid en zorgt ervoor dat telkens indien en voor zover dat mogelijk is de meest recente functionaliteit beschikbaar is voor opdrachtgever. Indien en voor zover de dienst echter bestaat uit maatwerk, garandeert SafeHarbour niet dat dit maatwerk blijft functioneren bij een nieuwe versie. Alvorens een nieuwe versie van de dienst beschikbaar te stellen, zal in dat geval SafeHarbour met opdrachtgever contact opnemen, en eventueel een voorstel uitbrengen voor het aanpassen van het maatwerk indien en voor zover dit nodig blijkt te zijn.

4.10. In het kader van de continuïteit van de informatievoorziening van de opdrachtgever zullen partijen, in het geval van beëindiging van de dienst, per omgaande in overleg treden omtrent de (wijze van) overdracht van data, de dienstverlening en/of overige beheersmaatregelen, benodigd voor een ongestoorde voortgang van het gebruik door opdrachtgever van haar data, programmatuur en/of dienst.

4.11. In het kader van overgang naar een andere leverancier zal SafeHarbour opdrachtgever in staat stellen een eventuele overgang te laten plaatsvinden.

4.12. Alle werkzaamheden die door SafeHarbour in het kader van artikel 4.9 tot en met 4.10 worden verricht worden op basis van nacalculatie tegen de dan geldende prijzen en tarieven in rekening gebracht.

4.13. Indien en voor zover een SaaS-dienst opdrachtgever de mogelijkheid biedt om materiaal te raadplegen, zoals bijvoorbeeld online (privacy)handboeken, dan geldt artikel Artikel 6 van deze algemene voorwaarden mutatis mutandis voor dat materiaal.

Artikel 5. Prijzen en tarieven, facturering en betaling

5.1. Alle prijzen en tarieven zijn aangegeven in euro's, exclusief omzetbelasting en exclusief overige van overheidswege opgelegde heffingen. Voor uitvoering van diensten of andere werkzaamheden buiten werkuren geldt een (spoed)toeslag welke wordt vastgelegd in de overeenkomst, of bij gebreke waarvan, de vigerende spoedprijzen en tarieven gelden.

5.2. Jaarlijks is SafeHarbour gerechtigd voor haar diensten de prijzen en tarieven te verhogen. Voor duurovereenkomsten geldt dat als de verhoging meer is dan drie (3) procent is ten opzichte van het voorgaande jaar, opdrachtgever het recht heeft de overeenkomst binnen 30 dagen na bekendmaking door SafeHarbour op te zeggen.

5.3. Alle facturen dienen door opdrachtgever betaald te worden binnen 30 (dertig) dagen na factuurdatum, tenzij anders is overeengekomen. Bij gebreke van betaling binnen de betalingstermijn is opdrachtgever -nadat deze door SafeHarbour is aangemaand waarbij opdrachtgever een redelijke termijn gegund is om alsnog te betalen- in gebreke, en heeft dit tot gevolg dat ook alle niet vervallen facturen terstond opeisbaar worden. Opdrachtgever is bovendien, zonder dat enige ingebrekestelling is vereist, de geldende wettelijke handelsrente over het factuurbedrag aan SafeHarbour verschuldigd.

5.4. Eventuele reclames op grond van vermeend onjuiste facturen of (vermeende) gebreken in de nakoming van de overeenkomst dienen schriftelijk binnen tien (10) dagen na factuurdatum respectievelijk uitvoering door SafeHarbour te zijn ontvangen, bij gebreke waarvan het recht op reclame op de betreffende factuur vervalt.

5.5. Indien en voor zover de overeenkomst het karakter heeft van een duurovereenkomst factureert SafeHarbour deze per kwartaal vooruit, tenzij uitdrukkelijk anders overeengekomen is.

Artikel 6. Intellectuele eigendomsrechten

6.1. Alle rechten van intellectuele eigendom op de op grond van de overeenkomst door SafeHarbour opgestelde of aan opdrachtgever ter beschikking gestelde (audit)rapporten, (kwaliteits)handboeken, analyses, ontwerpen, documentatie, offertes of andere werken waarop intellectuele eigendomsrechten kunnen berusten, evenals voorbereidend materiaal daarvan, berusten uitsluitend bij SafeHarbour, diens licentiegevers of diens toeleveranciers. Opdrachtgever verkrijgt uitsluitend een niet-exclusieve, niet aan derden overdraagbare en niet-sublicentieerbare licentie, welke niet meer inhoudt dan dat de werken mogen worden aangewend voor het doel waarvoor het is afgenomen. Het is opdrachtgever niet toegestaan werken van SafeHarbour aan derden ter beschikking te stellen.

6.2. Opdrachtgever garandeert dat geen rechten van derden zich verzetten tegen beschikbaarstelling aan SafeHarbour van apparatuur, programmatuur, (audit)rapporten, databestanden of andere materialen. Opdrachtgever vrijwaart SafeHarbour tegen elke aanspraak van een derde die gebaseerd is op de bewering dat zodanig beschikbaar stellen inbreuk maakt op enig recht van die derde.

Artikel 7. Geheimhouding

7.1. Informatie en/of documentatie is vertrouwelijk indien deze ofwel als zodanig door de ene partij is aangemerkt dan wel de andere partij anderszins weet of kan vermoeden dat informatie en/of documentatie vertrouwelijk is.

7.2. Partijen, en de personeelsleden van partijen, zullen vertrouwelijke informatie die is verkregen of ter beschikking gesteld door de andere partij uitsluitend gebruiken overeenkomstig het bepaalde in de overeenkomst en deze niet direct of indirect aan derden verstrekken, of hiertoe toestemming geven, zonder voorafgaande schriftelijke toestemming van de andere partij. Partijen, hieronder ook begrepen de personeelsleden van partijen, zullen voorts alle benodigde voorzorgsmaatregelen nemen om deze te beschermen tegen ongeautoriseerd gebruik en openbaarmaking.

7.3. Het gestelde in dit artikel geldt niet indien een partij vertrouwelijke informatie krachtens rechterlijke uitspraak of beschikking van overheidswege openbaar dient te maken.

7.4. Opdrachtgever zal ook na beëindiging van de overeenkomst alle vertrouwelijke informatie, of informatie waarvan zij kan of zou kunnen vermoeden dat deze vertrouwelijk is, tegenover derden geheimhouden. Voorts draagt opdrachtgever er zorg voor dat de hierboven bedoelde vertrouwelijke informatie onverwijld na beëindiging vernietigd wordt. Op eerste verzoek van SafeHarbour toont opdrachtgever aan dat dit daadwerkelijk gebeurd is.

7.5. Hetgeen in voorgaande leden van dit artikel is bepaald, is van overeenkomstige toepassing op de periode van voor de totstandkoming van de overeenkomst.

7.6. Elk der partijen zal gedurende de looptijd van de overeenkomst evenals één jaar na het einde daarvan slechts na voorafgaande schriftelijke toestemming van de andere partij, medewerkers van de andere partij die betrokken zijn of zijn geweest bij de uitvoering van de overeenkomst, in dienst nemen dan wel anderszins, direct of indirect, voor zich laten werken. Aan bedoelde toestemming kunnen voorwaarden zijn verbonden.

Artikel 8. Verwerking en bescherming van persoonsgegevens

8.1. De leden van dit artikel zijn alleen en integraal van toepassing op de SaaS-dienst zoals bedoeld in artikel 4.

8.2. SafeHarbour is gerechtigd de persoonsgegevens betreffende de opdrachtgever en/of gebruiker op te nemen in de persoonsregistratie van SafeHarbour welke benodigd is voor haar administratie- en beheerstaken.

8.3. In het kader van het verwerken van persoonsgegevens worden respectievelijk de volgende rollen onderscheiden en door partijen erkend (inclusief de daarbij behorende verantwoordelijkheden): de opdrachtgever is de verwerkingsverantwoordelijke, SafeHarbour wordt beschouwd als verwerker, eventueel door SafeHarbour ingeschakelde derde die persoonsgegevens verwerkt is sub-verwerker.

8.4. Eventuele persoonsgegevens zijn slechts toegankelijk voor SafeHarbour en ingeschakelde sub-verwerkers en worden niet aan andere derden verstrekt, tenzij SafeHarbour hiertoe krachtens de wet of een rechterlijke uitspraak verplicht is of wordt.

8.5. SafeHarbour verwerkt persoonsgegevens binnen de SaaS-dienst conform de Algemene Verordening Gegevensbescherming (hierna: AVG).

8.6. SafeHarbour legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen persoonsgegevens met zich meebrengen. De maatregelen zijn er mede op gericht om onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

8.7. SafeHarbour mag in het kader van de overeenkomst gebruik maken van een sub-verwerker. Opdrachtgever geeft hierbij bij voorbaat algemene toestemming voor het inschakelen van sub-vewerkers. Op eerste verzoek van opdrachtgever verstrekt SafeHarbour een lijst van sub-verwerkers. Deze lijst kan door SafeHarbour naar eigen inzicht en oordeel worden uitgebreid. Mocht SafeHarbour de lijst uitbreiden met nieuwe sub-verwerkers dan wordt Opdrachtgever hiervan tijdig op de hoogte gesteld, waarbij Opdrachtgever in de gelegenheid wordt gesteld om bezwaar te maken tegen de beoogde nieuwe sub-bewerkers.

8.8. Indien en voor zover het in voorgaand lid bedoeld bezwaar redelijk en gerond is, zullen SafeHarbour en opdrachtgever zoeken naar redelijke oplossingen om de bezwaren weg te nemen en aan de wensen tegemoet te komen. Mochten opdrachtgever en SafeHarbour niet tot een werkbare oplossing kunnen komen, dan is de opdrachtgever met inachtneming van een opzegtermijn van 30 (dertig) dagen gerechtigd de bewerkersovereenkomst en de overeenkomsten die hieraan gelieerd zijn en/of verband houden te beëindigen.

8.9. Opdrachtgever garandeert dat de inhoud, het gebruik en de opdracht tot de verwerkingen van de persoonsgegevens, niet onrechtmatig is en geen inbreuk maakt op enig recht van derden. Opdrachtgever vrijwaart SafeHarbour tegen alle aanspraken en claims die hiermee verband houden.

8.10. SafeHarbour garandeert aan een audit mee te zullen werken indien opdrachtgever wil vaststellen in hoeverre SafeHarbour voldoet aan haar verplichtingen ingevolge de Algemene Verordening Gegevensbescherming, zolang de kosten van de audit en de kosten die samenhangen met de inzet van medewerkers van SafeHarbour voor rekening van opdrachtgever zijn en blijven.

8.11. Indien SafeHarbour vermoedt, of te weten is gekomen, dat de persoonsgegevens van opdrachtgever gecompromitteerd zijn (security breach of een datalek), of zijn geweest, meldt SafeHarbour dit onverwijld aan opdrachtgever. Naar aanleiding daarvan beoordeelt opdrachtgever of zij de Autoriteit Persoonsgegevens en betrokkenen zal informeren of niet. Opdrachtgever blijft verantwoordelijk voor alle op hem rustende verplichtingen in dit kader. Voor zover noodzakelijk verleent SafeHarbour medewerking aan de opdrachtgever om te kunnen voldoen aan die wettelijke verplichtingen.

8.12. Opdrachtgever garandeert, zoals opgenomen in bijlage 2 en 3, intern passende technische en organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking, zoals bijvoorbeeld een adequaat wachtwoordenbeleid en een autorisatiestructuur die past bij de functies van gebruikers, waarbij opdrachtgever de verantwoordelijkheid heeft deze autorisatiestructuur zelf goed in de SaaS-dienst in te stellen.

8.13. In het geval dat een betrokkene een verzoek omtrent inzage, correctie of verwijdering richt aan SafeHarbour, of enig ander recht dat hem toekomt wenst uit te oefenen, zal SafeHarbour het verzoek doorsturen aan opdrachtgever, en zal opdrachtgever het verzoek verder afhandelen. SafeHarbour stelt de betrokkenen daarvan op de hoogte stellen. Voor zover niet in strijd met enige wettelijke bepaling zal desgevraagd SafeHarbour medewerking verlenen aan opdrachtgever bij de behandeling en afhandeling van het verzoek.

8.14. Na het verstrijken van de looptijd van de overeenkomst/opdracht of de gestelde verwerkingsduur van de persoonsgegevens dan wel beëindiging van de overeenkomst/opdracht zal SafeHarbour de opdrachtgever in gelegenheid stellen de persoonsgegevens te verkrijgen alvorens de persoonsgegevens te wissen.

8.15. Artikel 8.5 tot en met 8.14 geldt als een basisvewerkersovereenkomst tussen partijen. Op eerste verzoek van opdrachtgever werkt SafeHarbour mee aan het sluiten van een separate verwerkersovereenkomst.. Hiertoe levert SafeHarbour haar standaard model aan. Indien opdrachtgever van dat model wenst af te wijken of zij haar eigen model wenst te gebruiken, is SafeHarbour gerechtigd om de daarmee samenhangende kosten bij opdrachtgever in rekening te brengen. SafeHarbour garandeert niet dat zij met alle gewenste wijzigingen en/of bepalingen van opdrachtgever kan instemmen.

Artikel 9. Overdracht rechten en verplichtingen, onderaanneming

9.1. Opdrachtgever is niet gerechtigd rechten en verplichtingen aan een derde over te dragen, zonder dat voorafgaande schriftelijke toestemming is verkregen van SafeHarbour. De toestemming als hiervoor bedoeld kan niet door SafeHarbour niet op onredelijke gronden worden geweigerd.

9.2. SafeHarbour is gerechtigd bij de uitvoering van de opdracht gebruik te maken van derden, ongeacht of dat geschiedt op grond van onderaanneming of inhuur van personeel. SafeHarbour zal daarbij de geheimhoudingsverplichting zoals in voorgaand artikel is bepaald doorcontracteren aan deze derden.

9.3. SafeHarbour is gerechtigd om alle in het kader van de overeenkomst verworven rechten en plichten zonder enige aanvullende beperking aan derden over te dragen. Zij informeert opdrachtgever hierover zo spoedig mogelijk.

Artikel 10. Toerekenbare en niet-toerekenbare tekortkomingen

10.1. De totale aansprakelijkheid van SafeHarbour wegens een toerekenbare tekortkoming in de nakoming van de overeenkomst of uit enige andere hoofde, daaronder uitdrukkelijk ook begrepen iedere tekortkoming in de nakoming van een met opdrachtgever overeengekomen garantieverplichting, is beperkt tot vergoeding van directe schade tot maximaal het bedrag van de voor die

overeenkomst bedongen en door opdrachtgever daadwerkelijk betaalde prijs exclusief BTW. Indien de overeenkomst hoofdzakelijk een duurovereenkomst is, is de aansprakelijkheid beperkt tot directe schade en tot hetgeen door SafeHarbour in het kader van die overeenkomst opdrachtgever in de twee maanden aan de schadeveroorzakende gebeurtenis aan opdrachtgever exclusief BTW in rekening is gebracht en daadwerkelijk door opdrachtgever is betaald. In geen geval zal de totale aansprakelijkheid van SafeHarbour voor directe schade, uit welke hoofde dan ook, meer bedragen dan € 50.000 (vijftig duizend euro) voor een schadeveroorzakende gebeurtenis, waarbij een reeks opvolgende schadeveroorzakende gebeurtenissen geldt als één gebeurtenis.

10.2. De aansprakelijkheid van SafeHarbour voor indirecte schade, gevolgschade, gederfde winst, gemiste besparingen, verminderde goodwill, schade door bedrijfsstagnatie, schade als gevolg van aanspraken van afnemers van opdrachtgever, schade verband houdende met het gebruik van door opdrachtgever aan SafeHarbour voorgeschreven zaken, materialen of programmatuur van derden en schade verband houdende met de inschakeling van door opdrachtgever aan SafeHarbour voorgeschreven toeleveranciers is uitgesloten. Eveneens is uitgesloten de aansprakelijkheid van SafeHarbour wegens verminking, vernietiging of verlies van gegevens of documenten.

10.3. De hiervoor bedoelde uitsluitingen en beperkingen komen te vervallen indien en voor zover de schade het gevolg is van opzet of bewuste roekeloosheid van de bedrijfsleiding van SafeHarbour.

10.4. Tenzij nakoming door de SafeHarbour blijvend onmogelijk is, ontstaat de aansprakelijkheid van SafeHarbour wegens toerekenbare tekortkoming in de nakoming van een overeenkomst slechts indien opdrachtgever SafeHarbour onverwijld schriftelijk in gebreke stelt, waarbij een redelijke termijn voor de zuivering van de tekortkoming wordt gesteld, en SafeHarbour ook na die termijn toerekenbaar blijft tekortschieten in de nakoming van zijn verplichtingen. De ingebrekestelling dient een zo volledig en gedetailleerd mogelijke omschrijving van de tekortkoming te bevatten, opdat SafeHarbour in de gelegenheid wordt gesteld adequaat te reageren.

10.5. Iedere vordering tot schadevergoeding tegen SafeHarbour vervalt door het enkele verloop van drie (3) maanden na het ontstaan daarvan.

10.6. Het bepaalde in dit artikel alsmede alle andere beperkingen en uitsluitingen van aansprakelijkheid genoemd in deze algemene voorwaarden gelden mede ten gunste van alle (rechts)personen waarvan SafeHarbour zich bij de uitvoering van de overeenkomst bedient.

10.7. SafeHarbour is niet gehouden tot het nakomen van enige verplichting indien zij daartoe verhinderd is als gevolg van een omstandigheid die niet is te wijten aan haar schuld, noch krachtens wet, rechtshandeling of in het verkeer geldende opvattingen voor haar rekening komt of dient te komen. Indien SafeHarbour zich jegens opdrachtgever op overmacht beroept, zal SafeHarbour de opdrachtgever hieromtrent zo spoedig mogelijk, evenwel binnen een redelijke termijn, schriftelijk in kennis stellen.

10.8. Onder een niet toerekenbare tekortkoming (overmacht) voor SafeHarbour wordt in elk geval begrepen het niet naar behoren kunnen nakomen door SafeHarbour van haar verplichtingen ten gevolge van gebrek aan personeel, (langdurige) ziekte van haar personeel, stakingen, verkeersstremmingen, verlies van data en documenten, stroomstoringen, verlate aanlevering van zaken en/of diensten, zulks ongeacht of deze omstandigheid gelegen is of plaatsvindt bij SafeHarbour zelf of bij haar leverancier(s), ongeschiktheid van materialen, programmatuur en/of apparatuur waarvan het gebruik door opdrachtgever aan SafeHarbour door opdrachtgever is voorgeschreven.

10.9. Indien een overmachtsituatie langer dan zestig (60) dagen heeft geduurd en opdrachtgever SafeHarbour schriftelijk in gebreke heeft gesteld, heeft opdrachtgever het recht om de overeenkomst middels een aangetekend schrijven met onmiddellijke ingang buiten rechte te ontbinden, zonder dat SafeHarbour tot enige schadevergoeding is gehouden. Hetgeen reeds ingevolge de overeenkomst is gepresteerd wordt alsdan pro rato afgerekend. Voor vaststelling van wat reeds gepresteerd is, prevaleren de urenstaten uit het tijdschrijfsysteem van SafeHarbour.

Artikel 11. Looptijd, beëindiging en opschorting

11.1. De overeenkomst treedt in werking op het moment dat partijen ingevolge artikel 1 een overeenkomst zijn aangegaan, tenzij in de overeenkomst anders is overeengekomen. Als de overeenkomst geen duurovereenkomst betreft eindigt de overeenkomst zodra de verplichtingen van beide partijen over en weer in het kader van de uitvoering van de overeenkomst zijn uitgevoerd. Als de overeenkomst een duurovereenkomst betreft gelden de leden 2 tot en met 4 van dit artikel niet.

11.2. Een overeenkomst wordt aangegaan voor de duur zoals daarin is vermeld.

11.3. Indien in de overeenkomst geen looptijd is overeengekomen, geldt deze als aangegaan voor één (1) jaar, tenzij de aard van de overeenkomst zich daartegen verzet. In dat laatste geval blijkt uit de overeenkomst zelf wanneer deze eindigt.

11.4. Na ommekomst van de (initiële) looptijd van de overeenkomst wordt de overeenkomst verlengd voor een periode gelijk aan de initiële looptijd tenzij deze eindigt doordat de opdrachtgever deze schriftelijk opzegt met inachtneming van een opzegtermijn van dertig (30) dagen tegen het einde van de looptijd.

11.5. Indien overeenkomst is aangegaan voor onbepaalde tijd, is opdrachtgever gerechtigd deze op te zeggen door middel van een aangetekend schrijven, gericht aan SafeHarbour en met inachtneming van een opzegtermijn van dertig (30) dagen tegen het eind van een kalenderjaar. Opzegging kan niet eerder dan nadat de overeenkomst tenminste één (1) jaar heeft geduurd.

11.6. SafeHarbour is onverlet hetgeen in de overeenkomst is bepaald, gerechtigd de overeenkomst door een schriftelijke verklaring en zonder voorafgaande ingebrekestelling of kennisgeving, geheel of gedeeltelijk, met onmiddellijke ingang te ontbinden:

a. indien opdrachtgever toerekenbaar tekortschiet ter zake van één of meer van zijn verplichtingen en/of nakoming onmogelijk is;
b. indien voor SafeHarbour aannemelijk is dat opdrachtgever niet in staat of bereid is of zal zijn om aan haar verplichtingen te voldoen;
c. indien opdrachtgever surséance heeft aangevraagd, in de situatie van surséance verkeert, faillissement is aangevraagd, in staat van faillissement verkeert, overgaat tot liquidatie van zijn onderneming dan wel zijn activiteiten staakt of op enigerlei wijze insolvabel blijkt;
d. indien SafeHarbour door de samenwerking met opdrachtgever imagoschade leidt danwel een verdere samenwerking met opdrachtgever tot voorzienbare imagoschade van SafeHarbour zal leiden.

11.7. In geval van ontbinding als hiervoor bedoeld is SafeHarbour nimmer tot welke vorm van schadevergoeding ook gehouden. Opdrachtgever is gehouden SafeHarbour te vrijwaren van, en schadeloos te stellen ter zake vorderingen van derden die door of in verband met de ontbinding als in voorgaand lid bedoeld mochten ontstaan.

11.8. In geval van ontbinding als bedoeld in lid 6 is opdrachtgever gehouden alle reeds door SafeHarbour gemaakte kosten terstond te vergoeden, onverminderd het recht van SafeHarbour om volledige schadevergoeding te vorderen.

11.9. Indien partijen op het moment van ontbinding van een overeenkomst reeds prestaties ter uitvoering daarvan hebben verricht en ontvangen, dan zullen deze prestaties en daarmee samenhangende betalingsverplichtingen geen voorwerp van ongedaanmaking zijn. Dit ongeacht de reden van de ontbinding. Door SafeHarbour aan opdrachtgever uitgereikte facturen zijn op het moment van ontbinding direct opeisbaar.

11.10. Verplichtingen welke naar hun aard bestemd zijn om ook na beëindiging van de opdracht voort te duren, blijven bestaan. De beëindiging van de overeenkomst ontslaat partijen uitdrukkelijk niet van het bepaalde met betrekking tot: geheimhouding, intellectuele eigendomsrechten, toepasselijk recht en bevoegde rechter. Dit geldt ook bij beëindiging door ontbinding op basis van een toerekenbare tekortkoming van SafeHarbour.

Artikel 12. Toepasselijk recht, bevoegde rechter en overige bepalingen

12.1. Op alle offertes, overeenkomsten en uit overeenkomsten voortvloeiende overeenkomsten waarop deze voorwaarden van toepassing zijn en alle daaruit voortvloeiende rechtsbetrekkingen is uitsluitend Nederlands recht van toepassing.

12.2. Partijen laten hun geschillen bij voorkeur beslechten door middel van mediation van bij voorkeur de SGOA (Stichting Geschillen Oplossing Automatisering, zie http://www.sgoa.org).

12.3. Als partijen middels mediation niet tot een vergelijk kunnen komen met betrekking tot een geschil voortvloeiende uit of samenhangende met de overeenkomst zal het geschil worden voorgelegd aan de bevoegde rechter binnen het arrondissement Rotterdam.

12.4. Bovendien kunnen partijen zich in spoedeisende gevallen wenden tot de voorzieningenrechter van de daartoe bevoegde arrondissementsrechtbank om te oordelen in kort geding, of zich te wenden tot de daartoe bevoegde Arrondissementsrechtbank voor het nemen van conservatoire maatregelen.

12.5. Waar in onderhavige algemene voorwaarden gesproken wordt over “schriftelijk”, gelden elektronische berichten als e-mail en fax ook als schriftelijk. Tenzij er wordt gesproken over een aangetekend schrijven, in dat geval wordt ook daadwerkelijk een aangetekend schrijven per post bedoeld.

12.6. Bij strijdigheid tussen de bepalingen in deze algemene voorwaarden en/of de offerte prevaleert de opdrachtbevestiging boven deze algemene voorwaarden en prevaleren deze algemene voorwaarden boven de offerte.

***

Algemene Voorwaarden

Versie 1.3 van 16.8.2018

Bijlage 1 Auditing bij de algemene voorwaarden

Tijdens de Algemene Vergadering van de NOREA op 13 juli 2006 is ingestemd met de 'Code of Ethics voor IT-auditors' ter vervanging van het Reglement Gedrags- en Beroepsregels Register EDP-Auditors (GBRE). Deze Code of Ethics is gebaseerd op de Code of Ethics van de International Federation of Accountants (IFAC) en geldt met ingang van 14 juli 2006.

Gedragscode geldend voor iedere IT-auditor

Hoofdstukindeling:

A-100 Inleiding en fundamentele beginselen

A-110 Integriteit

A-120 Objectiviteit

A-130 Deskundigheid en zorgvuldigheid

A-140 Geheimhouding

A-150 Professioneel gedrag

Hoofdstuk A-100 Inleiding en fundamentele beginselen
Artikel A-100.1
De IT-auditor aanvaardt te allen tijde de verantwoordelijkheid op te treden in het algemeen belang en behartigt dientengevolge niet uitsluitend de belangen van een individuele opdrachtgever. Daartoe neemt de IT-auditor bij zijn optreden deze Code in acht en handelt in overeenstemming daarmee.

Artikel A-100.2
De IT-auditor maakt van het in deze Code beschreven conceptueel raamwerk gebruik bij het signaleren van een bedreiging. Hij evalueert een bedreiging naar aard en belang. Indien blijkt dat een bedreiging van niet te verwaarlozen betekenis is, treft de IT-auditor waarborgen die de bedreiging wegnemen of terugbrengen tot een aanvaardbaar niveau, zodat de naleving van de fundamentele beginselen geen geweld wordt aangedaan. De IT-auditor legt de bedreiging van niet te verwaarlozen betekenis, de naar aanleiding daarvan getroffen waarborgen en zijn conclusie vast.

Artikel A-100.3
Deze Code bevat de fundamentele beginselen van de beroepsethiek voor de IT-auditor, alsmede het conceptueel raamwerk voor de toepassing van deze fundamentele beginselen. Het conceptueel raamwerk geeft richting aan de toepassing van deze fundamentele beginselen.

Het NOREA-bestuur kan nadere regels uitvaardigen over de toepassing van het conceptueel raamwerk in specifieke situaties opdat waarborgen worden opgenomen die in aanmerking komen om een bedreiging weg te nemen of terug te brengen tot een aanvaardbaar niveau. Ook kunnen voorbeelden worden opgenomen van situaties waarin geen waarborgen beschikbaar zijn en van activiteiten of relaties die moeten worden vermeden.

Deze Code is van toepassing op iedere in het RE- register ingeschreven IT-auditor

Algemene Voorwaarden

Versie 1.3 van 16.8.2018

Fundamentele beginselen

Artikel A-100.4

De IT-auditor neemt de volgende fundamentele beginselen in acht:

a) Integriteit

De IT-auditor treedt in zijn beroepsmatige en zakelijke betrekkingen eerlijk en oprecht op.

b) Objectiviteit

De IT-auditor accepteert niet dat zijn professioneel of zakelijk oordeel wordt aangetast door een vooroordeel, belangentegenstelling of ongepaste beïnvloeding door een derde.
c) Deskundigheid en zorgvuldigheid

De IT-auditor houdt zijn deskundigheid en vaardigheid op het niveau dat is vereist om aan een opdrachtgever professionele diensten te kunnen verlenen in overeenstemming met actuele ontwikkelingen in de praktijk, wetgeving en vaktechniek. De IT-auditor handelt bij het verlenen van professionele diensten zorgvuldig en in overeenstemming met de van toepassing zijnde vaktechnische en overige beroepsvoorschriften.

d) Geheimhouding

De IT-auditor eerbiedigt het vertrouwelijke karakter van informatie die hij in het kader van zijn beroepsmatig en zakelijk handelen heeft verkregen. Hij maakt deze informatie zonder specifieke machtiging daartoe niet aan een derde bekend, tenzij wettelijk of beroepshalve een recht of plicht daartoe bestaat. Het is de IT-auditor niet toegestaan vertrouwelijke informatie die hij bij zijn beroepsmatig of zakelijk handelen heeft verkregen, te gebruiken om zichzelf of een derde te bevoordelen.

e) Professioneel gedrag

De IT-auditor houdt zich aan de voor hem relevante wet- en regelgeving en onthoudt zich van handelen dat het auditberoep in diskrediet brengt. Bij samenloop van functies dient een zodanige zorgvuldigheid in acht genomen te worden dat de relatie tussen het optreden c.q. het uiting geven als Register EDP-auditor en de andere functie ondubbelzinnig bepaald is.

Deze fundamentele beginselen zijn gedetailleerd besproken in de artikelen A-110 tot en met artikel A-150.

Conceptueel raamwerk

Artikel A-100.5
De IT-auditor handelt in overeenstemming met het conceptueel raamwerk bij iedere door hem gesignaleerde bedreiging die niet van te verwaarlozen betekenis is en bij de naar aanleiding daarvan getroffen waarborgen die deze bedreiging wegnemen of terugbrengen tot een aanvaardbaar niveau.

De omstandigheid waaronder de IT-auditor zijn werkzaamheden verricht kan leiden tot een bedreiging. Het is niet mogelijk iedere situatie te beschrijven waarin een bedreiging ontstaat en aan te geven welke waarborgen daartegen kunnen worden getroffen. Bovendien kunnen de aard van de opdrachten en van de uit te voeren werkzaamheden verschillen. Als gevolg daarvan kunnen ook verschillende en meerdere bedreigingen optreden waardoor het treffen van verschillende en meerdere waarborgen noodzakelijk is. Een conceptueel raamwerk dat van de IT-auditor vraagt iedere bedreiging te signaleren, te evalueren en aan de orde te stellen, in plaats van de eis te voldoen aan een aantal min of meer arbitraire specifieke regels, is in het algemeen belang. Deze Code biedt een raamwerk ter ondersteuning van de IT-auditor bij het signaleren en evalueren van iedere bedreiging en bij het in reactie daarop treffen van de juiste waarborgen.

Versie 1.3 van 16.8.2018

Artikel A-100.6
De IT-auditor evalueert omstandigheden of relaties waarmee hij bekend is of in redelijkheid bekend behoort te zijn, die de naleving van de fundamentele beginselen in gevaar kan brengen.

Artikel A-100.7
De IT-auditor betrekt bij het beoordelen van de aard, het belang en de ernst van een bedreiging zowel kwalitatieve als kwantitatieve factoren. Indien De IT-auditor niet in staat is adequate waarborgen te treffen weigert of beëindigt hij een opdracht tot het verlenen van een professionele dienst of beëindigt hij de opdrachtrelatie met de cliënt, dan wel zijn relatie met de organisatie waarbij of ten behoeve waarvan hij werkzaam is.

Artikel A-100.8
De IT-auditor kan onopzettelijk een bepaling uit deze Code schenden.
Indien dit het geval is, dan is het mogelijk, afhankelijk van de aard en de betekenis ervan, geen sprake van schending van de basisbeginselen mits de gevolgen onmiddellijk na ontdekking van de schending worden geëvalueerd, voor zover mogelijk gecorrigeerd en eventuele waarborgen worden getroffen.

Artikel A-100.9
De IT-auditor beperkt zich bij het toepassen van het conceptueel raamwerk niet tot de in deze Code opgenomen voorbeelden.

Bedreigingen en waarborgen

Artikel A-100.10
Het scala aan bedreigingen is groot. Een bedreiging valt doorgaans in één of meerdere van de volgende categorieën:

a. bedreiging als gevolg van eigenbelang: Dit is de bedreiging die ontstaat uit een financieel of ander belang van de IT-auditor dan wel van een gezins- of naast familielid van hem;
b. bedreiging als gevolg van zelftoetsing: Dit is de bedreiging die ontstaat indien de IT-auditor zijn eigen werkzaamheden of het resultaat daarvan beoordeelt;
c. bedreiging als gevolg van belangenbehartiging: Dit is de bedreiging die ontstaat indien de IT-auditor op een zodanige wijze een standpunt verdedigt dat objectiviteit in het gedrang komt;
d. bedreiging als gevolg van vertrouwdheid: Dit is de bedreiging die ontstaat indien er een nauwe band bestaat tussen de IT-auditor en zijn opdrachtgever of indien de IT-auditor te veel sympathie koestert voor de belangen van een ander;
e. bedreiging als gevolg van intimidatie: Dit is de bedreiging die ontstaat indien de IT-auditor door feitelijke of vermeende dreigementen wordt afgehouden van objectief handelen.

Artikel A-100.11

Waarborgen die een bedreiging wegnemen of tot een aanvaarbaar niveau terugbrengen zijn globaal in twee categorieën te verdelen:

a) waarborgen tot stand gebracht door de wetgever, de NOREA of andere regelgevers; en
b) waarborgen in de werkomgeving.

Artikel A-100.12
De waarborgen tot stand gebracht door de wetgever, de NOREA of andere regelgevers omvatten onder meer:

a. regelgeving ten aanzien van Corporate- en/of IT-Governance;
b. eisen voor inschrijving in het RE-register ter zake van, opleiding, ervaring en goed gedrag;
c. eisen ten aanzien van de permanente educatie;
d. vaktechnische en overige beroepsvoorschriften;
e. stelsel van kwaliteitsbeheersing;
f. externe beoordeling van de door de IT-auditor uitgevoerde assurance en daaraan verwante opdrachten;
g. klacht- en tuchtrecht.

Artikel A100.13

P.M.

Artikel A-100.14

Bepaalde waarborgen kunnen de kans vergroten dat onethisch gedrag wordt voorkomen of wordt ontdekt. Dergelijke waarborgen die kunnen zijn getroffen door de wetgever, de NOREA, andere regelgevers of de huishouding waaraan de IT-auditor is verbonden of waarbij hij werkzaam is, omvatten onder meer een effectieve en in ruime kring bekend gemaakte procedure, uitgevoerd door de werkgever, de NOREA of een regelgever, die het mogelijk maakt dat collega's, werkgevers of andere personen onprofessioneel of onethisch gedrag kunnen melden.

Versie 1.3 van 16.8.2018

Artikel A-100.15
In zijn professionele oordeelsvorming neemt de IT-auditor in aanmerking hetgeen een redelijk en goed geïnformeerde derde die over alle relevante informatie beschikt, waaronder de aard en het belang van de bedreiging en de getroffen waarborgen, als aanvaardbaar zal aanmerken.
De aard en het belang van de te treffen waarborgen zijn afhankelijk van de specifieke omstandigheden.

Oplossen van beroepsethische conflicten

Artikel A-100.16
Bij het beoordelen van het al dan niet naleven van de fundamentele beginselen is het mogelijk dat van de IT-auditor wordt verlangd dat hij een oplossing vindt voor een conflict over de toepassing van de fundamentele beginselen.

Artikel A-100.17

Indien de IT-auditor formeel dan wel informeel het initiatief neemt een conflict over de toepassing van de fundamentele beginselen op te lossen neemt hij de volgende aspecten, hetzij afzonderlijk, dan wel in hun onderlinge samenhang, in aanmerking:
a. de relevante feiten;
b. de relevante beroepsethische aspecten;
c. de fundamentele beginselen die van toepassing zijn op het conflict;
d. de geldende interne procedures; en
e. de mogelijke alternatieve handelwijzen.

Nadat de IT-auditor deze aspecten in aanmerking heeft genomen, kiest hij een adequate handelwijze overeenkomend met de in het geding zijnde fundamentele beginselen. Daarbij weegt de IT-auditor de gevolgen van de alternatieve handelwijzen tegen elkaar af.

Indien voor het conflict geen oplossing wordt gevonden vraagt de IT-auditor advies aan de daartoe aangewezen personen van de auditorganisatie waarbij hij werkzaam is of waaraan hij is verbonden of van de organisatie waarbij of ten behoeve waarvan hij werkzaam is.

Artikel A-100.18
Als de kwestie bestaat uit een conflict met of binnen een organisatie overweegt de IT-auditor daarnaast om degenen die zijn belast met het bestuur van of met het toezicht op die organisatie te raadplegen.
Hierbij kan gedacht worden aan de directie, Raad van Commissarissen of de audit commissie.

Artikel A-100.19
Het is in het belang van de IT-auditor de meest belangrijke aspecten van het conflict, de details van de gevoerde besprekingen en de daaromtrent genomen besluiten te documenteren.

Artikel A-100.20
Indien de IT-auditor een ernstig conflict niet kan oplossen, verdient het aanbeveling dat hij, zonder de vertrouwelijkheid geweld aan te doen, advies vraagt aan de NOREA (Raad voor Beroepsethiek) of aan een juridische adviseur.

Indien de IT-auditor bijvoorbeeld wordt geconfronteerd met een fraude waarvan bekendmaking kan leiden tot een bedreiging voor de naleving van de geheimhoudingsplicht, overweegt hij of het noodzakelijk is juridisch advies in te winnen om te bepalen of hij al dan niet verplicht is de fraude bij de daarvoor aangewezen instanties te melden.

Artikel A-100.21
Indien, nadat alle denkbare oplossingen in de beoordeling zijn betrokken, het niet mogelijk blijkt het beroepsethische conflict op te lossen, maakt de IT-auditor, indien mogelijk, een einde aan zijn betrokkenheid bij de aangelegenheid die heeft geleid tot het conflict.

Dit kan betekenen dat de IT-auditor, gezien de omstandigheden, moet besluiten zich uit het opdrachtteam terug te trekken, zijn medewerking aan een deelopdracht te beëindigen, zijn functie bij de opdracht neer te leggen of zijn relatie met de auditorganisatie of de organisatie waarbij of ten behoeve waarvan hij werkzaam is te verbreken of ontslag te nemen.

Hoofdstuk A-110 Integriteit

Artikel A-110-1
De IT-auditor treedt in zijn beroepsmatige en zakelijke betrekkingen eerlijk en oprecht op, doet eerlijk zaken en doet de waarheid geen geweld aan.

Artikel A-110.2
De IT-auditor vermijdt dat hij in verband wordt gebracht met informatie die naar zijn oordeel een bewering bevat die:

a. materieel onjuist of misleidend is;
b. op ongefundeerde gronden is gedaan;
c. niet volledig is of een verkeerde indruk wekt als gevolg waarvan de bewering als misleidend kan worden ervaren.

Versie 1.3 van 16.8.2018

Artikel A-110.3
De IT-auditor handelt niet in strijd met het bepaalde in artikel A-110.2 indien hij aan bedoelde informatie een mededeling toevoegt waarin hij zijn bezwaren tegen deze informatie tot uitdrukking brengt.

Hoofdstuk A-120 Objectiviteit

Artikel A-120.1
De IT-auditor accepteert niet dat zijn professioneel of zakelijk oordeel wordt aangetast door een vooroordeel, belangentegenstelling of ongepaste beïnvloeding door een derde.

Artikel A-120.2
De IT-auditor vermijdt iedere situatie die zijn professionele oordeelsvorming op een ongepaste wijze beïnvloedt.
De IT-auditor kan in een situatie komen te verkeren waarin zijn objectiviteit in het gedrang komt. Het is onmogelijk al deze situaties te beschrijven.

Hoofdstuk A-130 Deskundigheid en zorgvuldigheid

Artikel A-130.1
De IT-auditor houdt zijn deskundigheid en vaardigheid op het niveau dat is vereist om aan een opdrachtgever professionele diensten te kunnen verlenen in overeenstemming met actuele ontwikkelingen in de praktijk, wetgeving en vaktechniek. De IT-auditor handelt bij het verlenen van professionele diensten zorgvuldig en in overeenstemming met de van toepassing zijnde vaktechnische en overige beroepsvoorschriften.

Artikel A-130.2
Deskundige dienstverlening vereist van de IT-auditor een deugdelijke oordeelsvorming bij de toepassing zijn van professionele kennis en vaardigheid. Professionele deskundigheid kan worden verdeeld in twee verschillende fasen:
a. het verwerven van professionele deskundigheid; en
b. het in stand houden van professionele deskundigheid.

Artikel A-130.3
Voor het in stand houden van de professionele deskundigheid van de IT-auditor is kennis van en inzicht in de relevante vaktechnische en beroepsmatige ontwikkelingen vereist, alsmede van ontwikkelingen in het bedrijfsleven.

Permanente educatie stelt de IT-auditor in staat in de omgeving waarin hij beroepsmatig werkzaam is in continuïteit deskundig op te treden.

Artikel A-130.4
Zorgvuldigheid omvat de verantwoordelijkheid van de IT-auditor op te treden in overeenstemming met de eisen die gelden voor de uitvoering van een opdracht, te weten, toewijding, voldoende diepgang en tijdigheid.

Artikel A-130.5
De IT-auditor treft maatregelen die ervoor zorgen dat degenen die onder zijn verantwoordelijkheid werken de juiste opleiding hebben en onder adequaat toezicht staan.

Artikel A-130.6
De IT-auditor maakt indien daartoe aanleiding bestaat zijn opdrachtgevers of andere gebruikers van zijn professionele diensten attent op de inherente beperkingen die zijn verbonden aan zijn diensten. Aldus voorkomt hij dat een door hem gegeven oordeel wordt geïnterpreteerd als een feitelijke bewering.

Artikel A-130.7
Het bestuur kan nadere voorschriften geven aangaande het bepaalde in artikel A-130.1 t/m A-130.6 ten aanzien van permanente educatie, audit- en overige standaarden.

Hoofdstuk A-140 Geheimhouding

Artikel A-140.1
De IT-auditor onthoudt zich van:
a. het buiten de auditpraktijk waarbij hij werkzaam is of waaraan hij is verbonden of buiten de organisatie waarbij of ten behoeve waarvan hij werkzaam is, bekend maken van vertrouwelijke informatie, die hij in het kader van zijn beroepsmatig en zakelijk optreden heeft verkregen, tenzij hij is gemachtigd tot bekendmaking over te gaan of wettelijk dan wel beroepshalve daartoe een recht of plicht bestaat; en
b. het gebruikmaken van vertrouwelijke informatie die hij in het kader van zijn beroepsmatig en zakelijk handelen heeft verkregen om zichzelf of een derde te bevoordelen.

Artikel A-140.2
De IT-auditor houdt zich in zijn sociale omgang ook aan zijn geheimhoudingsplicht.
De IT-auditor is erop bedacht dat bij een langdurige omgang met een zakenrelatie, een gezinslid of een naast familielid de mogelijkheid bestaat onopzettelijk te handelen in strijd met zijn geheimhoudingsplicht.

Artikel A-140.3
De IT-auditor neemt zijn geheimhoudingsplicht ook in acht ter zake van informatie die hem ter beschikking is gesteld door een potentiële opdrachtgever.

Versie 1.3 van 16.8.2018

Artikel A-140.4
De IT-auditor overweegt de noodzaak de geheimhoudingsplicht in acht te nemen binnen de auditorganisatie waaraan hij is verbonden of waarbij hij werkzaam is of binnen de organisatie waarbij of ten behoeve waarvan hij werkzaam is.

Artikel A-140.5
De IT-auditor treft de redelijkerwijs te nemen maatregelen om te waarborgen dat de voor hem geldende geheimhoudingsplicht tevens in acht wordt genomen door personeelsleden die hiërarchisch aan hem ondergeschikt zijn en door personen aan wie hij om advies of ondersteuning vraagt.

Artikel A-140.6
De IT-auditor houdt zich aan zijn geheimhoudingsplicht ook na het beëindigen van de verbintenis met een cliënt of met een organisatie waarbij of ten behoeve waarvan hij werkzaam is.

Wanneer een IT-auditor van werkgever verandert of nieuwe opdrachten verwerft, is het hem toegestaan gebruik te maken van de bij zijn eerdere werkzaamheden verkregen kennis en opgedane ervaring. De vertrouwelijke informatie die De IT-auditor tijdens deze eerdere werkzaamheden heeft verkregen mag hij niet gebruiken of bekendmaken.

Artikel A-140.7
De IT-auditor kan in een situatie komen te verkeren waarin hij verplicht is of waarin het maatschappelijk juist is vertrouwelijke informatie bekend te maken. Voorbeelden hiervan zijn:

(a) bekendmaking is wettelijk toegestaan en door de opdrachtgever goedgekeurd;
(b) bekendmaking is wettelijk verplicht, bijvoorbeeld in geval van:

(i) de oplevering van documenten of levering van bewijs in het kader van een rechtsgeding;
(ii) de melding aan de geëigende overheidsinstanties van aan het licht gekomen schendingen van de wet; en

(c) de IT-auditor heeft een beroepsplicht, of is gerechtigd, tot bekendmaking, wanneer zulks niet bij wet verboden is:
(i) ter naleving van vaktechnische standaarden en ethische vereisten;
(ii) ter bescherming van de beroepsbelangen van een IT-auditor bij een rechtsgeding;
iii) teneinde medewerking te verlenen aan de kwaliteitsbeoordeling door de beroepsorganisatie; of
(iv) om te beantwoorden aan een verzoek om inlichtingen of een onderzoek door de beroepsorganisatie of een toezichthoudend lichaam.

Artikel A-140.8
Alvorens de IT-auditor besluit tot bekendmaking van vertrouwelijke informatie over te gaan betrekt hij in zijn besluitvorming:

a. in hoeverre de belangen van alle partijen, inclusief een derde waarvan de belangen in het spel zijn, kunnen worden geschaad in de situatie waarin een opdrachtgever de IT-auditor toestemming geeft tot het bekendmaken van de vertrouwelijke informatie;
b. in hoeverre alle relevante informatie bij hem bekend en voor zover uitvoerbaar, onderbouwd is. Indien het betreft het bekendmaken van onbewezen gegevens, onvolledige informatie of ongefundeerde conclusies, is professionele oordeelsvorming noodzakelijk om de wijze van bekendmaking vast te stellen; en
c de wijze van communicatie die wordt verwacht en degene aan wie deze wordt gericht. In het bijzonder overtuigt de IT-auditor zich ervan dat degene met wie wordt gecommuniceerd de juiste ontvanger is.

Hoofdstuk A-150 Professioneel gedrag

Artikel A-150.1
De IT-auditor houdt zich aan de voor hem relevante wet- en regelgeving en onthoudt zich van handelen dat het auditberoep in diskrediet brengt. Tot dit handelen behoren die handelingen die door een redelijke en goed geïnformeerde derde die over alle relevante informatie beschikt, zullen worden opgevat als schadelijk voor de goede naam van het auditberoep.

Artikel A-150.2
De IT-auditor brengt bij het zichzelf of zijn werk aanprijzen het auditberoep niet in diskrediet. De IT-auditor is eerlijk en oprecht in zijn promotionele activiteiten en onthoudt zich van:

a) het wekken van overdreven verwachtingen ter zake van de diensten die hij kan verlenen, de kwaliteiten die hij bezit en de ervaring waarover hij beschikt;
b) het maken van afkeurende verwijzingen naar of niet onderbouwde vergelijkingen met het werk van een derde.

Definities

a. IT-auditor: de Register EDP-auditor (RE), ingeschreven in het register van de NOREA;
b. NOREA, de Orde, de beroepsorganisatie: De Nederlandse Orde van Register EDP-auditors
c. auditorganisatie: de organisatorische eenheid waarbinnen één of meer IT-auditors professionele diensten verrichten;

d. bedreiging: het risico van het niet volledig naleven door de IT-auditor van één of meer van de fundamentele beginselen;
e. bestuur: het bestuur van de Nederlandse Orde van Register EDP-Auditors;
f. fundamentele beginselen: de beginselen integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag
g. opdracht: de tussen een opdrachtgever en auditorganisatie overeengekomen professionele dienst;
h. opdrachtgever: een cliënt waarmee de IT auditor een zakelijke relatie heeft, dan wel de organisatie waarmee de IT auditor een dienstverband heeft;
i. professionele dienst: de werkzaamheden van de IT-auditor waarvoor IT-auditdeskundigheid en deskundigheid op aanverwante terreinen is vereist.

Algemene Voorwaarden

Versie 1.3 van 16.8.2018

Bijlage 2 Verwerking van persoonsgegevens

Beschrijving doeleinden en wijze van Verwerking:

Overeenkomstig het bepaalde in de overeenkomst zal SafeHarbour de persoonsgegevens slechts en uitsluitend verwerken met het doel om gebruikers toegang te verlenen tot de SaaS-dienst om hen te helpen en ondersteunen bij het duurzaam verwerken en opslaan van kritische en privacygevoelige on- en offline data en informatie.

Categorieën van Betrokkenen:

Van de volgende categorieën personen zullen persoonsgegevens verwerkt worden:

- Gebruikers van een SaaS-dienst zijn vooral professionals uit de publieke sector.

Categorieën van Persoonsgegevens:

- E-mail
- Naam
- Functie
- Toegangsgegevens SaaS-dienst

Algemene Voorwaarden

Versie 1.3 van 16.8.2018

Bijlage 3 Beveiligingsmaatregelen

Om de persoonsgegevens te beveiligen zijn de volgende de technische en organisatorische beveiligingsmaatregelen door SafeHarbour getroffen:

Beleidsdocument voor informatiebeveiliging.

- Er is een beleidsdocument dat expliciet de maatregelen die verantwoordelijke treft om de verwerkte persoonsgegevens te beveiligen beschrijft.
- Dit beleidsdocument is goedgekeurd op bestuurlijk c.q. leidinggevend niveau en genoegzaam kenbaar gemaakt aan alle werknemers en relevante externe partijen.

Toewijzen van verantwoordelijkheden voor informatiebeveiliging.

- Alle verantwoordelijkheden die nodig zijn voor een adequate informatiebeveiliging zijn duidelijk gedefinieerd op zowel sturend als op uitvoerend niveau. Deze verantwoordelijkheden zijn belegd bij die verantwoordelijke personen die beveiligingsmaatregelen mogen en kunnen nemen.

Beveiligingsbewustzijn.

- Alle werknemers van SafeHarbour en, voor zover van toepassing, ingehuurd personeel en externe gebruikers worden getraind en regelmatig bijgeschoold over het informatiebeveiligingsbeleid en de informatiebeveiligingsprocedures van SafeHarbour.
- Tijdens de training en bijscholing wordt expliciet aandacht besteed aan de omgang met (bijzondere of anderszins gevoelige) persoonsgegevens.

Fysieke beveiliging en beveiliging van apparatuur.

- De IT-voorzieningen en apparatuur zijn fysiek beschermd tegen toegang door onbevoegden en tegen schade en storingen. De geboden bescherming is in overeenstemming met de vastgestelde risico's en het beveiligingsniveau dat volgens de wet- en regelgeving passend zou zijn.

Toegangsbeveiliging.

- Bij SafeHarbour gelden procedures om bevoegde gebruikers toegang te geven tot de informatiesystemen en -diensten die ze voor de uitvoering van hun taken nodig hebben en om onbevoegde toegang tot informatiesystemen te voorkomen.
- De procedures omvatten alle fasen in de levenscyclus van de gebruikerstoegang, van de eerste registratie van nieuwe gebruikers tot de uiteindelijke afmelding van gebruikers die niet langer toegang tot informatiesystemen en -diensten nodig hebben.
- Er wordt bijzondere aandacht besteed aan het beheren van toegangsrechten van gebruikers met extra ruime bevoegdheden, zoals systeembeheerders.

Logging en controle.

- Activiteiten die gebruikers uitvoeren met Persoonsgegevens zijn vastgelegd in logbestanden.
- Andere relevante gebeurtenissen, zoals pogingen om ongeautoriseerd toegang te krijgen tot Persoonsgegevens en verstoringen die kunnen leiden tot verminking of verlies van Persoonsgegevens zijn eveneens in logbestanden vastgelegd.
- De logbestanden worden periodiek gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van de persoonsgegevens en waar nodig wordt actie ondernomen.

Correcte verwerking in toepassingssystemen.

- In alle toepassingssystemen, inclusief toepassingen die door gebruikers zelf zijn ontwikkeld, zijn beveiligingsmaatregelen ingebouwd (privacy by design).
- Tot deze beveiligingsmaatregelen behoort de controle dat de invoer, de interne verwerking en de uitvoer aan vooraf gestelde eisen voldoen (validatie).
- Systeemdelen waarin gevoelige Persoonsgegevens worden verwerkt of die invloed hebben op de Verwerking van gevoelige Persoonsgegevens, zijn toegerust met aanvullende beveiligingsmaatregelen.

Algemene Voorwaarden

Versie 1.3 van 16.8.2018

Beheer van technische kwetsbaarheden.

- Software op servers van SafeHarbour, zoals browsers, virusscanners en operating systems, wordt up-to-date gehouden.
- Ook installeert SafeHarbour tijdig oplossingen die de leverancier uitbrengt voor beveiligingslekken in deze software.
- SafeHarbour verkrijgt tijdig informatie over technische kwetsbaarheden van de gebruikte informatiesystemen.
- SafeHarbour evalueert de mate waarin haar systeem blootstaat aan technische kwetsbaarheden.
- SafeHarbour treft tijdig geschikte maatregelen voor de behandeling van de risico's die samenhangen met het systeem.

Incidentenbeheer.

- SafeHarbour behandelt tijdig en doeltreffend informatiebeveiligingsincidenten en zwakke plekken in de beveiliging, zodra ze zijn gerapporteerd.
- SafeHarbour beoordeelt de risico's voor de betrokkenen en informeert effectief de betrokkenen en indien nodig ook de toezichthouder.
- De lessen getrokken uit de afgehandelde incidenten gebruikt SafeHarbour om de beveiliging waar mogelijk structureel te verbeteren.
- Als een vervolgprocedure na een informatiebeveiligingsincident juridische maatregelen omvat (civiel- of strafrechtelijk), wordt het bewijsmateriaal verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

Afhandeling van datalekken en beveiligingsincidenten.

- SafeHarbour meldt datalekken onmiddellijk aan Opdrachtgever (verwerkingsverantwoordelijke). De verwerkingsverantwoordelijke meldt dit lek zo spoedig mogelijk bij de betreffende toezichthouder.
- SafeHarbour informeert, indien daartoe verplicht of gehouden, ook de betrokkenen over het beveiligingsincident of het datalek.

Continuïteitsbeheer.

- SafeHarbour heeft in de organisatie continuïteitsbeheer ingericht om bij eventuele natuurrampen, ongevallen, uitval van apparatuur of opzettelijk handelen de gevolgen tot een aanvaardbaar niveau te beperken.
- Bij continuïteitsbeheer maakt SafeHarbour gebruik van een combinatie van preventieve maatregelen en herstelmaatregelen.