VERWERKERS-OVEREENKOMST

COMPO SOFTWARE BV

Bestaande uit:

Deel 1. Data Pro Statement

Deel 2. Standaardclausules voor verwerkingen

Versie *1.0 / 14 mei 2018.*

DEEL 1: DATA PRO STATEMENT

Dit Data Pro Statement vormt samen met de Standaardclausules voor verwerkingen de verwerkersovereenkomst voor het product of de dienst van het bedrijf dat dit Data Pro Statement heeft opgesteld.

ALGEMENE INFORMATIE

1. **Dit Data Pro Statement is opgesteld door:**

   COMPO Software b.v., gevestigd te 6269 AC Margraten, Rijksweg 44, KvK-nummer 14118403.
   Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met:
   Theo Breuers,
   Email: theo.breuers@composoftware.eu
   Tel.: (+31) 43 30 63 888

2. **Dit Data Pro Statement geldt vanaf 17 mei 2018 versie 1.0**

   De in dit Data Pro Statement omschreven beveiligingsmaatregelen passen wij regelmatig aan om ten aanzien van data protectie steeds voorbereid en actueel te blijven. Wij houden u op de hoogte van nieuwe versies via onze normale kanalen.

3. Dit Data Pro Statement is van toepassing op de volgende producten en diensten van data processor
   HR systeem Countable en de bijbehorende loonverwerking.

4. **Omschrijving product/dienst**
   Het product en de dienst zijn ontworpen om werkgevers tools aan te reiken op HR gebied en personeelsregistratie met als doel een juiste de salarisverwerking uit te voeren en maximale informatie te verstrekken aan de werkgevers en hun personeelsleden die gebruik maken van het systeem.

5. **Beoogd gebruik**
   Countable is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:
   Persoonsgegevens die noodzakelijk zijn voor salarisverwerking, optimale personeels-begeleiding optimalisering van de bedrijfsprocessen bij het inzetten van personeel.

   Bij het ontwerpen is rekening gehouden met de verwerking van bijzondere persoonsgegevens. Verwerken van deze gegevens met het hiervoor omschreven product of dienst door opdrachtgever is ter eigen beoordeling door opdrachtgever.

6. **Data processor heeft bij het ontwerpen van het product/de dienst *privacy by design* op de volgende wijze toegepast:**
   Klanten uploaden zelf de door hen te gebruiken gegevens, inclusief door hen gekozen bijlagen en kunnen deze gegevens en documenten wijzigen. Data processor controleert de gegevens niet en zal gegevens alleen inzien op verzoek van klant, bijvoorbeeld als dat nodig is om een vraag aan de helpdesk te beantwoorden of om gegevens verwijderen.

7. Data processor gebruikt de Data Pro Standaardclausules voor verwerkingen.

8. **Data processor verwerkt de persoonsgegevens van zijn opdrachtgevers** binnen **de EU/EER.**

9. **Data processor maakt gebruik van de volgende sub-processors:**

- Exconet BV
- Grutbroek 15b
- 7008 AK Doetinchem
- Hosting van de data in de cloud.
- ISO 9009, ISO 27001 en NEN 7510 gecertificeerd.

10. **Data processor ondersteunt opdrachtgever op de volgende manier bij verzoeken van betrokkenen:**
Het melden van storingen, correctie- en verwijderingsverzoeken kunnen worden aangevraagd worden per mail via onze helpdesk (helpdesk@composoftware.eu).
Bij spoed kan er overleg gepleegd worden via telefoonnummer (+31) 43 30 63 888).

11. **Na beëindiging van de overeenkomst met een opdrachtgever verwijdert data processor de persoonsgegevens die hij voor opdrachtgever verwerkt in principe binnen** 12 maanden **op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible).**
De termijn is langer dan 3 maanden om de klant na beëindiging van de overeenkomst nog inzage te geven in de opgeslagen data. Alleen inzien van de data is mogelijk. De data kunnen niet gewijzigd en/of verwijderd worden.
Op verzoek van de klant dan deze termijn verlengd worden.

BEVEILIGINGSBELEID

12. **Data processor heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn product of dienst:**
De vertrouwelijkheid en integriteit van het product worden geborgd doordat geheimhoudingsverklaringen zijn getekend door alle medewerkers van het bedrijf. De beschikbaarheid en de veerkracht van het product worden geborgd doordat het systeem in de cloud draait. Bij een incident wordt de beschikbaarheid en de toegang tot de persoonsgegevens tijdig hersteld door een back-up systeem.
De NCSC-NL matrix leidt tot een factor 15 en dat is volgens NCSC-NL een laag risico. De NCSC-NL matrix is als Deel 3 bijgevoegd.

13. **Data processor heeft zich geconformeerd aan het volgende Information Security Management System (ISMS):**
Geheimhoudingsverklaring voor alle medewerkers van de Data processor.

14. **Data processor werkt aan de volgende certificering:**
ISAE3402.

DATALEKPROTOCOL

15. In geval er toch iets mis gaat, hanteert data processor het volgende datalekprotocol om ervoor te zorgen dat opdrachtgever op de hoogte is van incidenten:

Data processor gebruikt de volgende monitoringtools/werkwijze om potentiele beveiligingsincidenten te signaleren: de sites met de daarbij behorende databases worden pro actief gecontroleerd en beveiligingsupdates worden direct uitgevoerd. Ook de subcontractor, Exonet BV waar de data gehost worden voert een proactief beleid ter voorkoming van data lekken. Er is een procedure voor het intern melden van incidenten. Indien de data processor in zijn organisatie een datalek ontdekt, zal de data processor zijn opdrachtgever daarvan zo snel mogelijk op de hoogte stellen, door contact op te nemen met de controller van opdrachtgever, door een email te sturen aan de controller van opdrachtgever.

Data processor levert zo veel mogelijk relevante gegevens aan, waaronder omschrijving van het incident, aard van de inbreuk, aard persoonsgegevens c.q. categorieën van betrokken data subjects, schatting van aantal betrokken data subjects en mogelijk betrokken databases, indicatie wanneer incident heeft plaatsgevonden (wat is er gebeurd?);

Contactgegevens contactpersoon (waar kan de controller met vragen terecht?);

Mogelijke gevolgen (wat kan er gebeuren, waar moet controller dan wel data subject op bedacht zijn, wijzen op mogelijkheden identiteitsfraude als gegevens als BSN nummers, inlog en wachtwoordgegevens, paspoort kopieën etc. in verkeerde handen terecht zijn gekomen);

Genomen maatregelen (wat heeft de data processor gedaan om eventuele schade te beperken of dit in de toekomst te voorkomen?);

Te nemen maatregelen door de controller dan wel betrokken data subjects (wat kunnen betrokken data subjects zelf doen, bijvoorbeeld “houd mail in de gaten, wijzig paswoorden;

Meldingen worden indien mogelijk binnen 2 uur gedaan aan opdrachtgevers. Data processor zal zelf geen meldingen doen aan AP of Data subjects. Wel of niet melden blijft de verantwoordelijkheid van de controller. De data processor zal de opdrachtgever of de controller desgewenst ondersteunen bij het meldproces.

DEEL 2: STANDAARDCLAUSULES VOOR VERWERKINGEN

versie: januari 2018

Vormt samen met het Data Pro Statement de verwerkersovereenkomst en is een bijlage bij de Overeenkomst en de daarbij behorende bijlagen zoals toepasselijke algemene voorwaarden

ARTIKEL 1. DEFINITIES

Onderstaande begrippen hebben in deze Standaardclausules voor verwerkingen, in het Data Pro Statement en in de Overeenkomst de volgende betekenis:

1.1 **Autoriteit Persoonsgegevens (AP):** toezichthoudende autoriteit, zoals omschreven in artikel 4, sub 21 Avg.

1.2 **Avg:** de Algemene verordening gegevensbescherming.

1.3 **Data Processor**: partij die als ICT-leverancier in het kader van de uitvoering van de Overeenkomst als verwerker Persoonsgegevens verwerkt ten behoeve van diens Opdrachtgever.

1.4 **Data Pro Statement**: statement van Data Processor waarin hij onder andere informatie geeft met betrekking tot het beoogd gebruik van zijn product of dienst, getroffen beveiligingsmaatregelen, subverwerkers, datalekken, certificeringen en omgang met rechten van Data subjects.

1.5 **Data subject (betrokkene)**: een geïdentificeerde of identificeerbare natuurlijke persoon.

1.6 **Opdrachtgever:** partij in wiens opdracht Data Processor persoonsgegevens verwerkt. De Opdrachtgever kan zowel verwerkingsverantwoordelijke (“controller”) zijn als een andere verwerker.

1.7 **Overeenkomst**: de tussen Opdrachtgever en Data Processor geldende overeenkomst, op basis waarvan de ICT-leverancier diensten en/of producten levert aan Opdrachtgever, waarvan de verwerkersovereenkomst onderdeel vormt.

1.8 **Persoonsgegevens**: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, zoals omschreven in artikel 4, sub 1 Avg, die Data Processor in het kader van de uitvoering van zijn verplichtingen voortvloeiende uit de Overeenkomst verwerkt.

1.9 **Verwerkersovereenkomst**: deze Standaardclausules voor verwerkingen, die tezamen met het Data Pro Statement (of vergelijkbare informatie) van Data Processor de verwerkersovereenkomst vormen als bedoeld in artikel 28, lid 3 Avg.

ARTIKEL 2. ALGEMEEN

2.1 Deze Standaardclausules voor verwerkingen zijn van toepassing op alle verwerkingen van Persoonsgegevens die Data Processor doet in het kader van de levering van zijn producten en diensten en op alle Overeenkomsten en aanbiedingen. De toepasselijkheid van verwerkersovereenkomsten van Opdrachtgever wordt uitdrukkelijk van de hand gewezen.

2.2 Het Data Pro Statement, en met name de daarin opgenomen beveiligingsmaatregelen, kan van tijd tot tijd door Data Processor worden aangepast aan veranderende omstandigheden. Data Processor zal Opdrachtgever van significante aanpassingen op de hoogte stellen. Indien Opdrachtgever in redelijkheid niet akkoord kan gaan met de aanpassingen, is Opdrachtgever gerechtigd binnen 30 dagen na kennisgeving van de aanpassingen de verwerkersovereenkomst schriftelijk gemotiveerd op te zeggen.

2.3 Data Processor verwerkt de Persoonsgegevens namens en in opdracht van Opdrachtgever overeenkomstig de met Data Processor overeengekomen schriftelijke instructies van Opdrachtgever.

2.4 Opdrachtgever, dan wel diens klant, is de verwerkingsverantwoordelijke in de zin van de Avg, heeft de zeggenschap over de verwerking van de Persoonsgegevens en heeft het doel van en de middelen voor de verwerking van de Persoonsgegevens vastgesteld.

2.5 Data Processor is verwerker in de zin van de Avg en heeft daarom geen zeggenschap over het doel van en de middelen voor de verwerking van de Persoonsgegevens en neemt derhalve geen beslissingen over onder meer het gebruik van de Persoonsgegevens.

2.6 Data Processor geeft uitvoering aan de Avg zoals neergelegd in deze Standaardclausules voor verwerkingen, het Data Pro Statement en de Overeenkomst. Het is aan Opdrachtgever om op basis van deze informatie te beoordelen of Data Processor afdoende garanties biedt met betrekking tot het toepassen van passende technische en organisatorische maatregelen opdat de verwerking aan de vereisten van de Avg voldoet en de bescherming van de rechten van Data subjects voldoende zijn gewaarborgd.

2.7 Opdrachtgever staat er tegenover Data Processor voor in dat hij conform de Avg handelt, dat hij zijn systemen en infrastructuur te allen tijde adequaat beveiligt en dat de inhoud, het gebruik en/of de verwerking van de Persoonsgegevens niet onrechtmatig zijn en geen inbreuk maken op enig recht van een derde.

2.8 Een aan Opdrachtgever door de AP opgelegde bestuurlijke boete kan niet worden verhaald op Data Processor, tenzij er sprake is van opzet of bewuste roekeloosheid aan de zijde van de bedrijfsleiding van Data Processor.

ARTIKEL 3. BEVEILIGING

3.1 Data Processor treft de technische en organisatorische beveiligingsmaatregelen, zoals omschreven in zijn Data Pro Statement. Bij het treffen van de technische en organisatorische beveiligingsmaatregelen heeft Data Processor rekening gehouden met de stand van de techniek, de uitvoeringskosten van de beveiligingsmaatregelen, de aard, omvang en de context van de verwerkingen, de doeleinden en het beoogd gebruik van zijn producten en diensten, de verwerkingsrisico's en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van Data subjects die hij gezien het beoogd gebruik van zijn producten en diensten mocht verwachten.

3.2 Tenzij expliciet anders vermeld in het Data Pro Statement is het product of de dienst van Data Processor niet ingericht op de verwerking van bijzondere categorieën van Persoonsgegevens of gegevens betreffende strafrechtelijke veroordelingen of strafbare feiten.

3.3 Data Processor streeft ernaar dat de door hem te treffen beveiligingsmaatregelen passend zijn voor het door Data Processor beoogde gebruik van het product of de dienst.

3.4 De omschreven beveiligingsmaatregelen bieden, naar het oordeel van de Opdrachtgever, rekening houdend met de in artikel 3.1 genoemde factoren een op het risico van de verwerking van de door hem gebruikte of verstrekte Persoonsgegevens afgestemd beveiligingsniveau.

3.5 Data Processor kan wijzigingen aanbrengen in de getroffen beveiligingsmaatregelen indien dat naar zijn oordeel noodzakelijk is om een passend beveiligingsniveau te blijven bieden. Data Processor zal belangrijke wijzigingen vastleggen, bijvoorbeeld in een aangepast Data Pro Statement, en zal Opdrachtgever waar relevant van die wijzigingen op de hoogte stellen.

3.6 Opdrachtgever kan Data Processor verzoeken nadere beveiligingsmaatregelen te treffen. Data Processor is niet verplicht om op een dergelijk verzoek wijzigingen door te voeren in zijn beveiligingsmaatregelen. Data Processor kan de kosten verband houdende met de op verzoek van Opdrachtgever doorgevoerde wijzigingen in rekening brengen bij Opdrachtgever. Pas nadat de door Opdrachtgever gewenste gewijzigde beveiligingsmaatregelen schriftelijk zijn overeengekomen en ondertekend door Partijen, heeft Data Processor de verplichting deze beveiligingsmaatregelen daadwerkelijk te implementeren.

ARTIKEL 4. INBREUKEN IN VERBAND MET PERSOONSGEGEVENS

4.1 Data Processor staat er niet voor in dat de beveiligingsmaatregelen onder alle omstandigheden doeltreffend zijn. Indien Data Processor een inbreuk in verband met Persoonsgegevens (zoals bedoeld in artikel 4 sub 12 Avg) ontdekt, zal hij Opdrachtgever zonder onredelijke vertraging informeren. In het Data Pro Statement (onder datalekprotocol) is vastgelegd op welke wijze Data Processor Opdrachtgever informeert over inbreuken in verband met Persoonsgegevens.

4.2 Het is aan de verwerkingsverantwoordelijke (Opdrachtgever, of diens klant) om te beoordelen of de inbreuk in verband met Persoonsgegevens waarover Data Processor heeft geïnformeerd gemeld moet worden aan de AP of Data subject. Het melden van inbreuken in verband met Persoonsgegevens, die op grond van artikel 33 en 34 Avg moeten worden gemeld aan de AP en/of Data subjects, blijft te allen tijde de verantwoordelijkheid van de verwerkingsverantwoordelijke (Opdrachtgever of diens klant). Data Processor is niet verplicht tot het melden van inbreuken in verband met persoonsgegevens aan de AP en/of de Betrokkene.

4.3 Data Processor zal, indien nodig, nadere informatie verstrekken over de inbreuk in verband met Persoonsgegevens en zal zijn medewerking verlenen aan noodzakelijke informatievoorziening aan Opdrachtgever ten behoeve van een melding als bedoeld in artikel 33 en 34 Avg.

4.4 Data Processor kan de redelijke kosten die hij in dit kader maakt in rekening brengen bij Opdrachtgever tegen zijn dan geldende tarieven.

ARTIKEL 5. GEHEIMHOUDING

5.1 Data Processor waarborgt dat de personen die onder zijn verantwoordelijkheid Persoonsgegevens verwerken een geheimhoudingsplicht hebben.

5.2 Data Processor is gerechtigd de Persoonsgegevens te verstrekken aan derden, indien en voor zover verstrekking noodzakelijk is ingevolge een rechterlijke uitspraak, een wettelijk voorschrift of op basis van een bevoegd gegeven bevel van een overheidsinstantie.

5.3 Alle door Data Processor aan Opdrachtgever verstrekte toegangs- en/of identificatiecodes, certificaten, informatie omtrent toegangs- en/of wachtwoordenbeleid en alle door Data Processor aan Opdrachtgever verstrekte informatie die invulling geeft aan de in het Data Pro Statement opgenomen technische en organisatorische beveiligingsmaatregelen zijn vertrouwelijk en zullen door Opdrachtgever als zodanig worden behandeld en slechts aan geautoriseerde medewerkers van Opdrachtgever kenbaar worden gemaakt. Opdrachtgever ziet erop toe dat zijn medewerkers de verplichtingen uit dit artikel naleven.

ARTIKEL 6. LOOPTIJD EN BEËINDIGING

6.1 Deze verwerkersovereenkomst maakt onderdeel uit van de Overeenkomst en iedere daaruit voortkomende nieuwe of nadere overeenkomst, treedt in werking op het moment van totstandkoming van de Overeenkomst en wordt gesloten voor onbepaalde tijd.

6.2 Deze verwerkersovereenkomst eindigt van rechtswege bij beëindiging van de Overeenkomst of enige nieuwe of nadere overeenkomst tussen partijen.

6.3 Data Processor zal, in geval van einde van de verwerkersovereenkomst, alle onder zich zijnde en van Opdrachtgever ontvangen Persoonsgegevens binnen de in het Data Pro Statement opgenomen termijn verwijderen op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (*render inaccessable*), of, indien overeengekomen, in een machine leesbaar formaat terugbezorgen Opdrachtgever.

6.4 Data Processor kan eventuele kosten die hij maakt in het kader van het in artikel 6.3 gestelde in rekening brengen bij Opdrachtgever. Hierover kunnen nadere afspraken worden neergelegd in het Data Pro Statement.

6.5 Het bepaalde in artikel 6.3 geldt niet indien een wettelijke regeling het geheel of gedeeltelijk verwijderen of terugbezorgen van de Persoonsgegevens door Data Processor belet. In een dergelijk geval zal Data Processor de Persoonsgegevens enkel blijven verwerken voor zover noodzakelijk uit hoofde van zijn wettelijke verplichtingen. Het bepaalde in artikel 6.3 geldt eveneens niet indien Data Processor verwerkingsverantwoordelijke in de zin van de Avg is ten aanzien van de Persoonsgegevens.

ARTIKEL 7. RECHTEN DATA SUBJECTS, DATA PROTECTION IMPACT ASSESSMENT (DPIA) EN AUDITRECHTEN

7.1 Data Processor zal, waar mogelijk, zijn medewerking verlenen aan redelijke verzoeken van Opdrachtgever die verband houden met bij Opdrachtgever door Data subjects ingeroepen rechten van Data subjects. Indien Data Processor direct door een Data subject wordt benaderd, zal hij deze waar mogelijk doorverwijzen naar Opdrachtgever.

7.2 Indien Opdrachtgever daartoe verplicht is, zal Data Processor na een daartoe redelijk gegeven verzoek zijn medewerking verlenen aan een gegevensbeschermingseffectbeoordeling (DPIA) of een daarop volgende voorafgaande raadpleging zoals bedoeld in artikel 35 en 36 Avg.

7.3 Data Processor kan de naleving van zijn verplichtingen op grond van de verwerkersovereenkomst aantonen door middel van een geldig Data Pro Certificaat of daaraan ten minste gelijkwaardig certificaat of auditrapport (Third Party Memorandum) van een onafhankelijke, deskundige.

7.4 Data Processor zal daarnaast op verzoek van Opdrachtgever alle verdere informatie ter beschikking stellen die in redelijkheid nodig is om nakoming van de in deze verwerkersovereenkomst gemaakte afspraken aan te tonen. Indien Opdrachtgever desondanks aanleiding heeft aan te nemen dat de verwerking van Persoonsgegevens niet conform de verwerkersovereenkomst plaatsvindt, dan kan hij maximaal éénmaal per jaar door een onafhankelijke, gecertificeerde, externe deskundige die aantoonbaar ervaring heeft met het soort verwerkingen dat op basis van de Overeenkomst wordt uitgevoerd, op kosten van de Opdrachtgever hiernaar een audit laten uitvoeren. De audit zal beperkt zijn tot het controleren van de naleving van de afspraken met betrekking tot verwerking van de Persoonsgegevens zoals neergelegd in deze Verwerkersovereenkomst. De deskundige zal een geheimhoudingsplicht hebben ten aanzien van hetgeen hij aantreft en zal alleen datgene rapporteren aan Opdrachtgever dat een tekortkoming oplevert in de nakoming van verplichtingen die Data Processor heeft op grond van deze verwerkersovereenkomst. De deskundige zal een afschrift van zijn rapport aan Data Processor verstrekken. Data Processor kan een audit of instructie van de deskundige weigeren indien deze naar zijn mening in strijd is met de Avg of andere wetgeving of een ontoelaatbare inbreuk vormt op de door hem getroffen beveiligingsmaatregelen.

7.5 Partijen zullen zo snel mogelijk in overleg treden over de uitkomsten in het rapport. Partijen zullen de voorgestelde verbetermaatregelen die in het rapport zijn neergelegd opvolgen voor zover dat van hen in redelijkheid kan worden verwacht. Data Processor zal de voorgestelde verbetermaatregelen doorvoeren voor zover deze naar zijn oordeel passend zijn rekening houdend met de verwerkingsrisico's verbonden aan zijn product of dienst, de stand van de techniek, de uitvoeringskosten, de markt waarin hij opereert, en het beoogd gebruik van het product of de dienst.

7.6 Data Processor heeft het recht om de kosten die hij maakt in het kader van het in dit artikel gestelde in rekening te brengen bij Opdrachtgever.

ARTIKEL 8. SUBVERWERKERS

8.1 Data Processor heeft in het Data Pro Statement vermeldt of, en zo ja welke derde partijen (subverwerkers) Data Processor inschakelt bij de verwerking van de Persoonsgegevens.

8.2 Opdrachtgever geeft toestemming aan Data Processor om andere subverwerkers in te schakelen ter uitvoering van zijn verplichtingen voortvloeiende uit de Overeenkomst.

8.3 Data Processor zal Opdrachtgever informeren over een wijziging in de door de Data Processor ingeschakelde derde partijen bijvoorbeeld middels een aangepast Data Pro Statement. Opdrachtgever heeft het recht bezwaar te maken tegen voornoemde wijziging door Data Processor. Data Processor draagt ervoor zorg dat de door hem ingeschakelde derde partijen zich aan eenzelfde beveiligingsniveau committeren ten aanzien van de bescherming van de Persoonsgegevens als het beveiligingsniveau waaraan Data Processor jegens Opdrachtgever is gebonden op grond van het Data Pro Statement.

ARTIKEL 9. OVERIG

Deze Standaardclausules voor verwerkingen vormen tezamen met het Data Pro Statement een integraal onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst, waaronder begrepen de van toepassing zijnde algemene voorwaarden en/of beperkingen van aansprakelijkheid, zijn derhalve ook van toepassing op de verwerkersovereenkomst.

DEEL 3: NCSC-NL MATRIX.

Wat is de NCSC-NL matrix?

De beveiligingsadviezen van NCSC-NL bevatten een inschaling van de beschreven kwetsbaarheid. Per advies wordt een Kans op uitbuiting en Schade bij uitbuiting gedefinieerd. De mogelijke waarden per onderdeel zijn Low, Medium of High. Voor zowel de Kans als Schade inschalingen wordt een set vragen beantwoord, die leiden tot een waarde. Wanneer er specifieke omstandigheden zijn, kan worden afgeweken van de matrix en kan de waarde voor Kans en/of Schade worden veranderd. Kwetsbaarheden waarvan zowel de Kans als de Schade als Low wordt ingeschaald, worden niet uitgestuurd.

Kans

De kans wordt bepaald door onderstaande vragen te beantwoorden en de waarde toe te kennen die achter elke optie staat.

Vraag	Optie 1		Optie 2		Optie 3	
Is de kwetsbaarheid aanwezig in de standaard configuratie/installatie?	Nee	1	Onduidelijk/Ja	3		
Is er Exploitcode beschikbaar?	Geen	1	Proof of Concept (PoC)	4	Exploit	6
Zijn er technische details beschikbaar	Geen	1	Enigszins	2	Volledig	3
Vereiste toegang	Fysiek	1	LAN/directe omgeving	4	internet	6
Vereiste credentials?	Admin	1	User	2	Geen	4
Hoe complex is het technisch gezien om de kwetsbaarheid uit te buiten?	Complex	1	Gemiddeld	2	Eenvoudig	3
Is er gebruikersinteractie nodig?	Complex	1	Eenvoudig	3	Geen	4
Wordt de kwetsbaarheid in het wild uitgebuit?	Nee	1	Beperkt	2	Grootschalig	3
Wordt de kwetsbaarheid, naar verwachting, op korte termijn misbruikt of verschijnt er een exploit?	Nee	1	Ja	3		
Beschikbaarheid oplossing?	Ouder dan 2 maanden	1	Tot 2 maand oud	2	Geen	3

Verklaring van de kans vragen:

Is de kwetsbaarheid aanwezig in de standaard configuratie/installatie?: Wanneer de kwetsbaarheid zich in een specifieke configuratie-instelling of installatie bevindt, is de kans dat een systeem kwetsbaar is minder groot dan wanneer de kwetsbaarheid standaard aanwezig is.

Is er Exploitcode beschikbaar?

Hoe minder een aanvaller hoeft te doen om systemen te kunnen compromitteren, hoe hoger de kans dat dit ook gebeurt.

Zijn er technische details beschikbaar:
Hoe meer technische details beschikbaar zijn, hoe (relatief) eenvoudiger het wordt om een exploit te schrijven wat de kans dat deze verschijnt vergroot. Mogelijke waarden zijn:

- Geen: er zijn geen details over de kwetsbaarheid gepubliceerd.
- Enigszins: er is een aantal details gepubliceerd. Het is bekend welke component of functie een probleem bevat en onder welke omstandigheden de kwetsbaarheid aanwezig is.
- Volledig: het exacte commando binnen de kwetsbare functie bekend is gemaakt, of kwetsbaarheid is aangetoond in de broncode.

Vereiste toegang:
De kans dat een kwetsbaar systeem wordt gecompromitteerd wanneer het toegankelijk is voor een beperkte groep mensen is kleiner dan wanneer het rechtstreeks vanaf het internet benaderbaar is. Mogelijke waarden zijn:

- Fysiek/Directe omgeving: de aanvaller moet fysiek in de buurt van het systeem zijn of met een gebruikersaccount kunnen inloggen.
- LAN: De aanvaller moet via het LAN netwerkverkeer kunnen sturen naar het kwetsbare systeem.
- Internet: Diensten zoals een webserver of een mailserver zullen worden aangemerkt als benaderbaar via het internet.

Vereiste credentials:
Wat voor gebruikersrechten heeft de aanvaller nodig om de kwetsbaarheid te kunnen uitbuiten?

Hoe complex is het technisch gezien om de kwetsbaarheid uit te buiten
Een kwetsbaarheid die eenvoudig uit te buiten is zal mogelijk eerder tot een werkende exploit leiden dan een technisch zeer complex probleem.
Is er gebruikersinteractie nodig?:
Moet de gebruiker worden overgehaald om een document te openen of een website te bezoeken?

Wordt de kwetsbaarheid in het wild uitgebuit?:
Wordt actief misbruikt op het internet? Is er sprake van grootschalig misbruik? Of een gerichte aanval?

Wordt de kwetsbaarheid binnenkort misbruikt of verschijnt er een exploit?
Deze vraag kent een gevoelswaarde toe aan de inschaling.

Beschikbaarheid oplossing:
Wanneer er geen oplossing bekend is, is het zeer interessant voor aanvallers om de kwetsbaarheid uit te buiten.
Door bovenstaande waarden toe te kennen aan de antwoorden ontstaat een kanswaarde per kwetsbaarheid. Op basis van discussiesessies en meerdere proefwegingen is bepaald dat de onderstaande verdeling wordt gehanteerd om een betrouwbare inschaling te doen.
Low: 10 – 18
Medium: 19 – 27
High: 28 – 38

Schade

De schade wordt bepaald door een van de onderstaande schadeomschrijvingen te kiezen. Wanneer meer dan één type schade kan worden veroorzaakt, wordt de zwaarste inschaling gebruikt.

Schadeomschrijving

Denial of Service (DoS):

De kwetsbaarheid kan ertoe leiden dat een dienst niet meer bereikbaar/bruikbaar is.

Uitvoeren van willekeurige code:

Na uitbuiting kan code of systeemcommando's worden uitgevoerd.

Rechten op afstand (remote (root-) shell):

Na uitbuiten van de kwetsbaarheid krijgt de aanvaller toegang tot een interactieve (root-)shell op afstand.

Verwerven lokale admin/root-rechten (privilege escalation):

Een reguliere gebruiker kan zich verhoogde rechten toe-eigenen door het uitbuiten van de kwetsbaarheid op het lokale systeem.

Lekkage informatie:

Door een kwetsbaarheid uit te buiten kan systeeminformatie of data buit worden gemaakt.

Vraag	Optie 1		Optie 2		Optie 3	
Denial of Service	Nee	Low	Ja, Client	Low	Ja, Infrastructuur dienst	High
Uitvoeren van willekeurige code	Nee	Low	Ja, Gebruikers rechten	Medium	Ja, Root / Administrator rechten	High
Rechten op afstand (remote (root-) shell)	Nee	Low	Ja, remote shell	Medium	Ja, remote root-shell	High
Verwerven lokale admin/root-rechten (privilege escallation)	Nee	Low	Ja	Medium		
Lekkage informatie	Nee	Low	Ja, systeem informatie	Medium	Ja, data	High