Leeuwenbrug 87a
7411 TH Deventer

Tel.: 024-3297772
Kamer van Koophandel nr. 69612447
BTW NL 8579 39 968 B01
IBAN NL52 RABO 0323 0041 72

CyberManager verwerkersovereenkomst

Ref: - IRM360 CyberManager Algemene Verwerkersovereenkomst v1.8.docx

1. Verwerkersovereenkomst

1.1. Inleiding

- Deze Verwerkersovereenkomst beschrijft de afspraken over de aard, duur, beveiliging, geheimhoudingsplicht, privacy rechten en audits m.b.t. het verwerken van persoonsgegevens door Verwerker IRM360 (de Leverancier) in opdracht van Verwerkingsverantwoordelijke Opdrachtgever (de Klant).
- Verwerker IRM360 levert diensten aan Verwerkingsverantwoordelijke Opdrachtgever (de Klant) betreffende het leveren van de SaaS toepassing CyberManager.
- Deze Verwerkersovereenkomst vormt samen met de getekende overeenkomst tussen Verwerker IRM360 (de Leverancier) en Verwerkingsverantwoordelijke Opdrachtgever (de Klant) één geheel en is onlosmakelijk verbonden met de CyberManager SaaS licentieovereenkomst (https://www.cybermanager.nl/cybermanager-saas-overeenkomst/) en kan niet los opgezegd worden door zowel Verwerker IRM360 (de Leverancier) als Verwerkingsverantwoordelijke Opdrachtgever (de Klant).

1.2. Artikel 1 - Duur van de overeenkomst

1) De aanvang en looptijd van deze Verwerkersovereenkomst is gelijk aan de aanvang en looptijd van de CyberManager overeenkomst.
2) Deze overeenkomst kan niet tussentijds worden opgezegd.
3) De bepalingen zoals omschreven in artikel 4 (Naleving) blijven ook na afloop van deze overeenkomst van kracht.

1.3. Artikel 2 - Onderwerp van de overeenkomst

1) De Verwerker verwerkt persoonsgegevens in opdracht van Verwerkingsverantwoordelijke in het kader van de CyberManager SaaS-dienst zoals beschreven in de dienstbeschrijving, zie Bijlage 2.
2) De Verwerker verbindt zich om in het kader van die werkzaamheden de door de Verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens zorgvuldig te verwerken.
3) De Verwerkingsverantwoordelijke heeft de plicht, voortvloeiend uit de AVG, om ervoor zorg te dragen dat de Verwerker voldoende waarborgen kent ten aanzien van de technische- en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen.

1.4. Artikel 3 - Het doel van de verwerking

1) Het leveren van de CyberManager SaaS-dienst
2) De verwerking en het bewaren van persoonsgegevens vindt enkel plaats in het kader van de navolgende doelstellingen:
    - Registratie van contactgegevens (NAW-gegevens en e-mailadres) van ingevoerde CyberManager gebruikers en/of medewerkers en overige contactpersonen of contactgegevens van leveranciers en betrokkenen die in de CyberManager door een

beheerder met het recht gebruikersbeheer worden ingevoerd (beheerder is eigenaar van deze informatie inzake de toegang, inhoud, onderhoud en verwijdering).

- De software en de gegevens die in de software worden opgeslagen, zullen worden beheerd door de beheerder van de SaaS-dienst. Deze taken zullen worden verricht door IRM360 of een door haar ingeschakelde sub-verwerker.

1.5. Artikel 4 - Naleving

1) De Verwerker verwerkt gegevens ten behoeve van de Verwerkingsverantwoordelijke, in overeenstemming met diens instructies.
2) De Verwerker heeft geen zeggenschap over de ter beschikking gestelde persoonsgegevens. Zo neemt hij geen beslissingen over ontvangst en gebruik van de gegevens, de invoer, de verstrekking aan derden en de duur van de opslag van gegevens. De zeggenschap over de persoonsgegevens verstrekt onder deze Verwerkersovereenkomst komt nimmer bij de Verwerker te berusten.
3) De Verwerker zal bij de verwerking van persoonsgegevens in het kader van de in artikel 3 genoemde werkzaamheden, handelen in overeenstemming met de toepasselijke wet- en regelgeving betreffende de bescherming van persoonsgegevens. De Verwerker verwerkt persoonsgegevens slechts in opdracht van de contactpersoon van Verwerkingsverantwoordelijke en zal alle redelijke instructies van dat kennisveld dienaangaande opvolgen, behoudens afwijkende wettelijke verplichtingen.
4) De Verwerker zal onmiddellijk en uiterlijk binnen 24 uur na het ontstaan van het incident, bij het ontdekken van beveiligingsinbreuken of datalekken, deze melden aan de betreffende Verwerkingsverantwoordelijke, al dan niet onder verbeurte van een boete in geval van niet- nakoming, conform artikel 10 van deze Verwerkersovereenkomst.
5) De Verwerker zal te allen tijde op eerste verzoek van de medewerker van de Verwerkingsverantwoordelijke onmiddellijk alle persoonsgegevens met betrekking tot deze Verwerkersovereenkomst ter hand stellen voor zover Verwerker toegang heeft tot de in artikel 3 genoemde dienst. Deze toegang is de eindverantwoordelijkheid van de Eindverantwoordelijke.
6) De Verwerker stelt de Verwerkingsverantwoordelijke te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG, meer in het bijzonder de rechten van betrokkenen, zoals, maar niet beperkt tot een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens en het uitvoeren van een gehonoreerd aangetekend verzet.
7) De Verwerker zal de persoonsgegevens niet aan derden verstrekken, tenzij dit gebeurt in opdracht van de Verwerkingsverantwoordelijke of wanneer dit noodzakelijk is om te voldoen aan een wettelijke verplichting.
8) Doorgifte naar landen buiten de EER is niet toegestaan zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke. Verwerkingsverantwoordelijke kan de toestemming aan nadere voorwaarden verbinden. Verwerker zal aan Verwerkingsverantwoordelijke melden in welke land of landen de persoonsgegevens worden verwerkt.

1.6. Artikel 4 - Geheimhouding

1) De Verwerker treft alle noodzakelijke maatregelen om geheimhouding van de persoonsgegevens van de Verwerkingsverantwoordelijke te waarborgen.

2) De in lid 1 gestelde verplichting geldt niet wanneer de Verwerkingsverantwoordelijke voorafgaand schriftelijke toestemming heeft gegeven om de persoonsgegevens aan een derde te verstrekken of wanneer de Verwerker hiertoe wettelijk verplicht is.
3) De Verwerker zal dezelfde geheimhoudingsplicht opleggen aan diens personeel c.q. hiervoor ingeschakelde personen of sub-Verwerkers.
4) Bij overtreding van dit artikel, verbeurt de Verwerker een onmiddellijk opeisbare boete van € 5.000 per overtreding aan de verantwoordelijke, onverminderd het recht van verantwoordelijke om volledige schadevergoeding te vorderen.

1.7. Artikel 5 - Beveiliging

1) De Verwerkingsverantwoordelijke en de Verwerker zullen beiden passende technische en organisatorische maatregelen treffen, zoals bedoeld in artikel 32 AVG, zodat zij een op het risico afgestemd beveiligingsniveau kunnen waarborgen.
2) De Verwerker houdt bij het treffen van beveiligingsmaatregelen rekening met de stand van de techniek, de uitvoeringskosten, alsook met de aard, omvang, context, verwerkingsdoeleinden, waarschijnlijkheid en ernst van de uiteenlopende risico's voor de rechten en vrijheden van personen een en ander conform het bepaalde in artikel 28 lid 3 sub f AVG.
3) Indien de Verwerkingsverantwoordelijke een beoordeling wenst uit te voeren van een beoogde verwerkingsactiviteit, verleent de Verwerker alle redelijke medewerking om deze beoordeling in overeenstemming met de geldende wet- en regelgeving uit te voeren.
4) De Verwerker verleent eveneens alle redelijke medewerking aan verzoeken van de Autoriteit Persoonsgegevens (en vergelijkbare buitenlandse toezichthouders) en aan een voorafgaande raadpleging van de Autoriteit Persoonsgegevens.
5) Partijen hebben in Bijlage 1 concrete afspraken gemaakt omtrent de voor de uitvoering van deze overeenkomst noodzakelijke technische en organisatorische beveiligingsmaatregelen, welke de verantwoordelijke op dit moment passend acht.
6) Deze afspraken omvatten ten minste de volgende onderwerpen:
    - de betrouwbaarheidseisen
    - het overeengekomen beveiligingsniveau (indien van toepassing)
    - de maatregelen getroffen door de Verwerker zodat uitsluitend bevoegd personeel toegang heeft tot de persoonsgegevens
    - maatregelen ter bescherming zoals tegen verlies, wijziging, onbevoegde of onrechtmatige verwerking, toegang of openbaarmaking
    - de te nemen maatregelen voor het opsporen van zwakke plekken en incidentenbeheer
7) Partijen zullen de in lid 7 en 8 genoemde afspraken periodiek evalueren en zo nodig aanpassen.
8) Deze beveiligingsmaatregelen zijn in Bijlage 1 nader omschreven.

1.8. Artikel 6 - Audit

1) De Verwerkingsverantwoordelijke heeft het recht om jaarlijks op eigen kosten een audit te laten uitvoeren ter controle op de naleving van deze overeenkomst. De kosten van de audit komen voor rekening van Verwerker indien uit de audit blijkt dat Verwerker

toerekenbaar tekort is geschoten in de nakoming van zijn verplichtingen op grond van de Verwerkersovereenkomst.

2) De Verwerker zal aan de in lid 1 genoemde audit alle redelijke medewerking verlenen, zoals het verlenen van toegang tot de databases en het ter beschikking stellen van alle relevante informatie.
3) De Verwerker voert de aanbevelingen die uit de audit zijn gekomen in overleg met de verantwoordelijke zo spoedig mogelijk uit.
4) Indien aanpassingen als gevolg van lid 3 voortkomen uit gewijzigde inzichten of wetgeving, dan zijn de redelijke kosten voor deze aanpassingen voor de verantwoordelijke.
5) Indien de aanpassingen als gevolg van lid 3 voortkomen uit een tekortkoming in de nakoming van de overeengekomen beveiligingseisen, dan zijn deze kosten voor de Verwerker.
6) Indien de Autoriteit Persoonsgegevens of een andere bevoegde autoriteit een onderzoek wenst uit te voeren, verleent de Verwerker daartoe alle redelijke medewerking en stelt hij de Verwerkingsverantwoordelijke hieromtrent zo snel mogelijk van op de hoogte.

1.9. Artikel 7 - Datalek

1) De Verwerker is verplicht te monitoren of zich een datalek of een inbreuk op de beveiliging (hierna samen: datalek) voordoet.
2) Indien zich een security incident en mogelijk datalek voordoet geldt de procedure meldplicht datalekken zoals vermeld in Bijlage 3 van deze overeenkomst. In geval van een datalek treft de Verwerker alle redelijke noodzakelijke maatregelen om de gevolgen hiervan te beperken en een nieuw lek te voorkomen.
3) Verwerker stelt Verwerkingsverantwoordelijke onmiddellijk op de hoogte indien naar zijn oordeel instructies in strijd zijn met de AVG of anderszins onredelijk zijn
4) De Verwerker verleent de Verwerkingsverantwoordelijke alle medewerking die noodzakelijk is om de omvang en gevolgen van het datalek te kunnen beoordelen en te kunnen voldoen aan de eventuele meldplicht datalekken richting de Autoriteit Persoonsgegevens alsook aan de informatieplicht richting betrokkenen.
5) Partijen hebben hun afspraken over de te volgen procedure in geval van een datalek vastgelegd in een procedure meldplicht datalekken, zoals omschreven in Bijlage 3. Deze procedure kan worden aangepast indien de stand van de techniek dit verlangt of de regelgeving omtrent de meldplicht datalekken wijzigt.

1.10. Artikel 8 – Overdracht en wijzigingen

1) Partijen dragen rechten en verplichtingen voortvloeiende uit deze Verwerkersovereenkomst niet over aan een derde zonder toestemming van de andere partij.
2) Verwerker zal bij gewijzigde omstandigheden die noodzakelijk zijn voor naleving van toepasselijke (Europese) wet- en regelgeving of van de door de Autoriteit Persoonsgegevens en de European Data Protection Board meest recent gepubliceerde richtsnoeren, opinies en beleidsregels maatregelen nemen.

1.11. Artikel 9 - Verzoeken van betrokkenen

1) Ieder verzoek tot inzage, rectificatie, gegevensverwijdering, beperking van de verwerking, overdraagbaarheid van gegevens of bezwaar zoals bedoeld in artikelen 15 tot en met 21 AVG dat de Verwerker bereikt, stuurt hij onverwijld door aan de verantwoordelijke.
2) De Verwerker verleent de Verwerkingsverantwoordelijke alle redelijke medewerking zodat laatstgenoemde binnen de wettelijke termijnen kan voldoen aan een verzoek zoals bedoeld in lid 1.
3) De Verwerkingsverantwoordelijke zal de redelijke kosten die een dergelijke medewerking met zich meebrengt aan de Verwerker vergoeden.

Het bepaalde in dit artikel is uitsluitend van toepassing in geval van kennelijk ongegronde of buitensporige verzoeken, waaronder begrepen herhaaldelijke verzoeken om informatieverstrekking door een betrokkene.

1.12. Artikel 10 - Sub-Verwerkers

1) De Verwerker is niet gerechtigd om Sub-Verwerkers in te schakelen voor het verwerken van de persoonsgegevens uit deze overeenkomst, tenzij hij hiervoor voorafgaande schriftelijke toestemming heeft gekregen. Verwerkingsverantwoordelijke geeft hierbij toestemming voor de in Bijlage 4 genoemde Sub-Verwerkers.
2) De Verwerker is verantwoordelijk en aansprakelijk voor de handelingen van door hem ingeschakelde Sub-Verwerkers.
3) Indien een Verwerker een Sub-Verwerker inschakelt is hij verplicht te bedingen dat deze sub-Verwerker alle bij deze overeenkomst opgelegde verplichtingen aan de Verwerker nakomt en zal daartoe met de betreffende Sub-Verwerkers een overeenkomst sluiten die in overeenstemming is met deze overeenkomst.
4) Indien de Verwerker zonder toestemming zoals bedoeld in lid 1 Sub-Verwerkers inschakelt, is de Verwerker een boete verschuldigd van € 500 onverminderd het recht van de verantwoordelijke op volledige schadevergoeding. Verwerker staat in voor een correcte naleving van deze plichten door deze subverwerkers en is bij fouten van deze subverwerkers zelf aansprakelijk voor alle schade die daardoor wordt veroorzaakt.

1.13. Artikel 11 - Toegang tot de persoonsgegevens

De Verwerker zorgt ervoor dat de Verwerkingsverantwoordelijke te allen tijde toegang houdt tot de betreffende persoonsgegevens, zelfs in geval van zijn faillissement of surseance van betaling.

1.14. Artikel 12 – Aansprakelijkheid en vrijwaring

1) De Verwerker is niet verantwoordelijk voor schade als gevolg van schendingen van enige wet- of regelgeving door de Verwerkingsverantwoordelijke.
2) De Verwerkingsverantwoordelijke vrijwaart de Verwerker voor aanspraken van derden en door Verwerker gemaakte kosten als gevolg van een schending zoals bedoeld in lid 1, met uitzondering van een situatie waarin de schending van wet- en regelgeving door de

verwerkersverantwoordelijke redelijkerwijs aan een daad verwerker kan worden toegewezen.

3) De Verwerkingsverantwoordelijke is niet verantwoordelijk voor schade als gevolg van schendingen van enige wet- of regelgeving door de Verwerker.
4) De Verwerker is aansprakelijk voor schade en kosten die Verwerkingsverantwoordelijke lijdt wegens een toerekenbare tekortkoming of onrechtmatige daad van Verwerker. Verwerker vrijwaart Verwerkingsverantwoordelijke voor schade en kosten wegens aanspraken van derden en/of door toezichthouders opgelegde boetes of sancties, die het gevolg zijn van een schending van enige wet- of regelgeving, dan wel het niet nakomen door Verwerker van enige verplichting uit deze Verwerkersovereenkomst.
5) De andere partij, is in een geval als bedoeld in lid 1 of 3, gerechtigd de hoofdovereenkomst met onmiddellijke ingang op te zeggen.

1.15. Artikel 13 – Beëindiging en gevolgen van beëindiging

1) Deze overeenkomst eindigt pas nadat de onderliggende opdracht is beëindigd en de Verwerker alle aan hem verstrekte persoonsgegevens heeft overgedragen aan de Verwerkingsverantwoordelijke of aan een door verantwoordelijke voorafgaand schriftelijk aangewezen derde, alsook alle achtergebleven gegevens bij de Verwerker en diens eventuele Sub-Verwerkers zijn vernietigd.
2) Op verzoek van de Verwerkingsverantwoordelijke stelt de Verwerker de aan hem verstrekte persoonsgegevens ter beschikking in een ander formaat dan waarin ze zijn aangeleverd tegen vergoeding van de redelijke kosten hiervan.
3) In plaats van overdraging van de gegevens kan de Verwerkingsverantwoordelijke de Verwerker ook verzoeken om de gegevens te vernietigen.
4) Vernietiging van de gegevens zoals bedoeld in lid 3 kan pas plaatsvinden nadat de Verwerkingsverantwoordelijke hiervoor voorafgaande schriftelijke toestemming heeft gegeven.
5) De bepalingen van artikel 4 (Naleving) blijven echter onverminderd van kracht.
6) Verwerker zal ervoor zorgdragen dat zij na de retournering of vernietiging alle verwerkingen van de deze overeenkomst betreffende persoonsgegevens onmiddellijk staakt en gestaakt houdt. Verwerker zal Verwerkingsverantwoordelijke op eerste verzoek een schriftelijke bevestiging en garantie daarvan verlenen en Verwerkingsverantwoordelijke toestaan om te verifiëren dat de betreffende persoonsgegevens niet langer worden verwerkt door Verwerker of een door haar ingeschakelde sub-verwerker, hulppersoon of andere derde.

1.16. Artikel 14 - Gevolgen van nietigheid of vernietigbaarheid

Indien een deel van de overeenkomst nietig of vernietigbaar is, dan tast dit de overige bepalingen in de overeenkomst niet aan. Een bepaling die nietig of vernietigbaar is, wordt in dat geval vervangen door een bepaling die het dichtst in de buurt komt van wat partijen bij het sluiten van de overeenkomst op dat punt voor ogen hadden.

1.17. Artikel 15 - Toepasselijk recht en bevoegde rechter

1) Op deze overeenkomst is Nederlands recht van toepassing.
2) Alle eventuele geschillen die ontstaan naar aanleiding van deze overeenkomst en die niet in der minne kunnen worden opgelost worden voorgelegd aan de bevoegde rechter in het arrondissement van de vestigingsplaats van de Verwerker.

Deze verwerkingsovereenkomst wordt actief na het akkoord gaan met de SAAS-overeenkomst.

IRM360

Marcel Lavalette

2. Bijlagen

2.1. Bijlage 1 - Beveiligingsmaatregelen

De volgende organisatorische maatregelen zijn door IRM360 B.V. genomen om het CyberManager platform te beveiligen.

1. Pseudonimisering en versleuteling van persoonsgegevens.
2. Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en privacy van de verwerkingssystemen en diensten te garanderen.
3. Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen.
4. Op gezette tijdstippen worden middels audits en/of kwetsbaarheden analyses de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking getest, beoordeeld en geëvalueerd.
5. Maatregelen om te waarborgen dat enkel bevoegde medewerkers toegang hebben tot de persoonsgegevens voor de doeleinden zijn genomen.
6. Maatregelen waarbij de Verwerker zijn medewerkers en Sub-Verwerkers uitsluitend toegang geeft tot persoonsgegevens via op naam gestelde accounts, waarbij het gebruik van die accounts adequaat gelogd wordt en waarbij de betreffende accounts alleen toegang geven tot die persoonsgegevens waartoe de toegang voor de betreffende (rechts)persoon noodzakelijk is;
7. Maatregelen om de persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag, verwerking, toegang of openbaarmaking.
8. Maatregelen om zwakke plekken te identificeren ten aanzien van de verwerking van persoonsgegevens in de systemen die worden ingezet voor het leveren van diensten aan Verwerkingsverantwoordelijke.
9. Maatregelen om de tijdige beschikbaarheid van de persoonsgegevens te garanderen.
10. Maatregelen om te waarborgen dat de persoonsgegevens logisch gescheiden worden verwerkt van de persoonsgegevens die Verwerker voor zichzelf of namens derde partijen verwerkt.

Om bovenstaande concreet te implementeren is een managementsysteem geborgen binnen de IRM360 B.V. organisatie volgens de ISO 27001 standaard voor informatiebeveiliging en is het hierin beschreven Information Security Management System (ISMS) geïmplementeerd.

2.2. Bijlage 2 – Dienstbeschrijving CyberManager

CyberManager SaaS platform
Gegevens die worden bewaard en verwerkt zijn enkel voor de registratie en verwerking van het managementplatform voor informatiebeveiliging, privacy en cybersecurity.

Verwerkingen
De verwerking en het bewaren van persoonsgegevens vindt enkel plaats in het kader van de navolgende doelstellingen: contactgegevens van ingevoerde CyberManager gebruikers en/of medewerkers. De gebruiker/klant is eigenaar van deze informatie inzake de inhoud, onderhoud en verwijdering en overige contactpersonen of contactgegevens van geïnteresseerden. In het laatste geval zal dit door ons bewaard worden naar gelang de afhandeling van de aanvraag afgehandeld is.

- (NAW): Deze genoemde persoonsgegevens worden enkel bewaard en verwerkt voor zover dat noodzakelijk is met het oog op de doelstellingen zoals opgenomen in dit privacy statement.
- (E-mail): Deze persoonsgegevens worden als inlognaam gebruikt
- (Overige): Gegevens als datum indiensttreding is verplicht om een actieve gebruiker te identificeren. Een datum uitdiensttreding kan optioneel ingevoerd worden.
- Persoonsgegevens die door Verwerkingsverantwoordelijke worden opgeslagen in CyberManager, waaronder persoonsgegevens die zijn opgenomen in het verwerkingsregister van Verwerkingsverantwoordelijke en registraties van incidenten en eventuele datalekken.

IRM360 B.V. en Sub-Verwerkers
IRM360 B.V. zorgt voor de (door)ontwikkeling en het onderhoud van de CyberManager, dit in samenspraak met eventuele partners en/of gebruikers. Met het oog op deze taken zal IRM360 B.V. zich actief bezighouden met de werking van de CyberManager.

IRM360 B.V en de door haar eventueel ingeschakelde Sub-Verwerkers hebben slechts toegang tot de persoonsgegevens binnen CyberManager indien en voor zover dat voor voornoemde taken (zoals onderhoud) strikt noodzakelijk is. Tussen IRM360 B.V. en de Sub-Verwerkers is overeengekomen dat zij ten aanzien van de persoonsgegevens strikte geheimhouding zullen betrachten. IRM360 B.V. en de Sub-Verwerkers zullen onder geen beding op onwettige wijze persoonsgegevens aan derden verstrekken.

2.3. Bijlage 3 – Datalek procedure

Voor de afhandeling van incidenten (zoals inbreuken op de beveiliging) en datalekken gelden de volgende regels.

Procedure melden datalekken
Bij constatering van een security incident, datalek of een vermoedelijk datalek aan de kant van de verwerker, moet dat direct worden gemeld aan de Information Security Officer.
Dit kan door een mail te sturen aan support@IRM360.nl.

De melding moet tenminste de volgende gegevens bevatten:

- de aard van de inbreuk (dus: wat is er gebeurd?);
- de oorzaak van het datalek (hack, diefstal, verlies, etc.);
- beschrijving van de gelekte persoonsgegevens (aard van de gegevens, hoeveelheid, etc.);
- eventuele maatregelen die genomen zijn/worden genomen om het datalek te dichten;
- een inschatting van het risico dat de betrokkenen kunnen lopen;
- contactgegevens van de melder.

De meldplicht aan de Information Security Officer van IRM360 B.V. geldt niet alleen voor medewerkers van IRM360 B.V., maar ook voor klanten, leveranciers en partners, voor zover die persoonsgegevens verwerken als Verantwoordelijke of Verwerker.

Melding aan AP en betrokkenen
De Information Security Officer onderzoekt, samen met de Information Security Officer of de Privacy Officer van Verwerkingsverantwoordelijke, naar aanleiding van de interne melding of er sprake is van een datalek. Zo ja, dan meldt Verwerkingsverantwoordelijke het datalek 'onverwijld' (uiterlijk op de tweede werkdag na het ontstaan van het incident) aan het Meldpunt Datalekken van de AP. Deze melding wordt niet door Verwerker (IRM360) maar door Verwerkingsverantwoordelijke gedaan via het op de website van de AP gepubliceerde meldformulier.

De Information Security Officer informeert de IRM360 B.V. directie en overige relevante afdelingen of Verwerkers over het data-lek, de verwerkersverantwoordelijk en de melding aan de AP. IRM360 B.V. zal geen melding doen aan de AP van datalekker waar zij geen verantwoordelijke is.

De Information Security Officer stelt vervolgens samen met de Information Security Officer of de Privacy Officer van Verwerkingsverantwoordelijke en in overleg met de relevante afdelingen vast of het datalek een 'aanmerkelijk risico op verlies of onrechtmatige verwerking waaraan nadelige gevolgen voor de persoonsgegevens en de persoonlijke levenssfeer van de betrokkene(n) zijn verbonden" tot gevolg heeft. Als daar sprake van is, worden de betrokkenen niet door Verwerker (IRM360) maar door Verwerkingsverantwoordelijke geïnformeerd over het datalek.

De melding aan betrokkenen is niet nodig indien de persoonsgegevens versleuteld of onbegrijpelijk zijn gemaakt, waardoor deze niet te lezen zijn door anderen. Dit moet van geval tot geval beoordeeld worden door Verwerkingsverantwoordelijke, omdat de effectiviteit van de versleuteling mede afhangt van het gebruikte algoritme en het moment/punt waarop de gegevens zijn versleuteld.

De berichtgeving aan betrokkenen kan door plaatsing van een bericht op de website en/of via een brief/e-mail aan betrokkenen, een en ander ter beoordeling van Verwerkingsverantwoordelijke, in overleg met de directie van IRM360. De kennisgeving aan betrokkenen moet in ieder geval de volgende informatie bevatten:

- de aard van de inbreuk in verband met persoonsgegevens

- een telefoonnummer of webpagina waar meer informatie over de inbreuk kan worden verkregen
- aanbevelingen om mogelijke negatieve gevolgen van de inbreuk voor betrokkenen te beperken.

Bijhouden overzicht
De Information Security Officer van IRM360 en de Information Security Officer of Privacy Officer van Verwerkingsverantwoordelijke houdt een overzicht bij van de datalekken, met daarin onder meer de gevolgen van de datalekken en de herstelmaatregelen die zijn genomen. Dit overzicht mag uitsluitend de voor dit doel noodzakelijke gegevens bevatten.

2.4. Bijlage 4 – Toegestane Sub-Verwerkers

Hieronder staan de door Verwerkingsverantwoordelijke toegestane sub-verwerkers

Naam sub-verwerker	Doel verwerking	Opmerking
Iland Nederland B.V.	Hosting CyberManager	Verwerkersovereenkomst aanwezig
Isatis Group	Financiële administratie en human resources	Verwerkersovereenkomst aanwezig