# DATA Pro Statement
# Optimum ICT

Versie 2024 nr 2.1
Auteur: Richard Janssen
Datum definitief: 10 mei 2024

Data Pro Code, NLDigital
Adherence ID: 2024SCOPE11003001DATAPRO
Public Register van de Data Pro Coede: https://scope-europe.eu/en/data-pro-code/public-register

**Optimum ICT B.V.**
Oud-Eemnesserweg 5-J
3741 MP Baarn
The Netherlands
T (+31) 88 747 7300

**Purmerend Office**
Boterbloem 49
1441 TV Purmerend
The Netherlands
T (+31) 88 747 7300

info@optimumict.nl
www.optimumict.nl
IBAN: NL69 INGB 0004 2708 52
VAT: NL8190.59.110.B01
CoC/KvK Amersfoort: 32107862

**INHOUDSOPGAVE**

## INLEIDING

Dit Data Pro Statement is onderdeel van de ondertekende offerte en/of overeenkomst tussen klant en Optimum ICT en de van toepassing zijnde Algemene Leveringsvoorwaarden (NLDigital Voorwaarden 2020).

In dit Statement en de Algemene leveringsvoorwaarden zijn de AVG vereisten verwerkt en uitgewerkt. De uitwerking van de vereisten zijn gebaseerd op de Data Pro Code van de ICT Brancheverenigingen NLDigital. Onderhavige uitwerking van de vereisten is conform de voorgeschreven nummering (1 t/m 17) uit de Data Pro Code.

De Data Pro Code wordt onafhankelijk getoetst door SCOPE Europe. Voldoen aan de code door Optimum ICT wordt gepubliceerd in het publieke Data Pro Register.

In dit Statement wordt afgeweken van sommige termen gebruikt in de standaard Data Pro code teksten. De door Optimum ICT gebruikte termen hebben dezelfde betekenis als bedoeld in de code:

| Data Pro Code | Statement Optimum |
|---|---|
| Data Processor | Verwerker |
| Opdrachtgever | Klant |
| Product of Dienst | Dienst |
| Sub-processor | Subverwerker |

De in het statement gebruikte geel gearceerde tekstgedeeltes zijn opties in de inrichting en uitvoering van de dienst. Deze gedeeltes worden aangepast zover nodig en in overleg met Klant, op basis van hun wensen.

## ALGEMENE INFORMATIE

### 1. Dit Data Pro Statement is opgesteld door de volgende verwerker:

Optimum ICT B.V., gevestigd aan de Oud-Eemnesserweg 5j, 3741 MP Baarn.

Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met:

Richard Janssen
Operationeel Manager
e-mail: privacy@optimumict.nl
Telefoonnummer: 088-7477300

### 2. Dit Data Pro Statement versie 2024 nr 2.0 geldt vanaf 14 februari 2024

Dit Data Pro Statement en de daarin 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 diensten van Verwerker:

| Diensten A t/m G |
|---|
| A. Microsoft Office 365 |
| B. Microsoft Office 365 – Exchange Online |
| C. Microsoft Office 365 – SharePoint Online & OneDrive voor Bedrijven |
| D. Backup Online |
| E. Router, firewall en (draadloos) netwerk |
| F. Laptops & computers |
| G. Server/centrale netwerkopslag |

## STATEMENT

### 4. Omschrijving product/dienst

| Uitwerking per dienst |
| --- |
| **A. Microsoft Office 365**<br><br>Office 365 is een verzameling van online diensten welke door Microsoft gehost wordt op een geografisch redundant uitgevoerd datacentrum in Europa. Met Office 365 beschikken bedrijven over een set panklare ICT oplossingen voor samenwerking en communicatie die relevant zijn voor de zakelijke gebruiker. Het platform voldoet aan strenge veiligheidsnormen en industrie standaarden voor compliancy, zoals ISO/IEC 270001.<br><br>Klant kan zelf gegevens uploaden, inclusief door hen gekozen bijlagen en kan gegevens en bestanden wijzigen en/of verwijderen.<br><br>Verwerker 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. |
| **B. Microsoft Office 365 – Exchange Online**<br><br>Voor zowel interne als externe communicatie via e-mail wordt er gebruik gemaakt van Exchange Online. De inhoud van mailboxen wordt gesynchroniseerd naar computers en mobiele apparaten zoals smartphones en tablets van Klant. |
| **C. Microsoft Office 365 – SharePoint Online & OneDrive voor Bedrijven**<br><br>Algemene kantoordocumenten en overige bestanden van Klant worden vastgelegd in SharePoint Online. Persoonlijke (zakelijke) bestanden kunnen gebruikers opslaan in OneDrive voor Bedrijven. Medewerkers kunnen evt. bestanden synchroniseren naar of bewerken op lokale apparaten zoals laptops en smartphones. |
| **D. Backup Online**<br><br>Backup Online wordt toegepast om een extra externe kopie te hebben van de voor Klant relevante data. De gegevens die worden vastgelegd kunnen afkomstig zijn van servers, laptops, mailboxen, SharePoint en/of OneDrive. In geval van een calamiteit op locatie bij Klant, defecte apparatuur of onbedoeld verwijderen van gegevens, kunnen deze worden teruggehaald uit een eerder gemaakte backup.<br><br>OPTIE: Er wordt geen additionele backup gemaakt van SharePoint Online, OneDrive en/of Exchange Online. |
| **E. Router, firewall en (draadloos) netwerk**<br><br>Op locatie bij Klant is een firewall actief welke beheerd wordt door Verwerker. De optie voor draadloze netwerktoegang is geleverd en geconfigureerd door Verwerker.<br>OPTIE: Op locatie bij Klant is een firewall actief welke niet geleverd is maar wel beheerd wordt door Verwerker. De optie voor draadloze netwerktoegang is geconfigureerd door Verwerker. |

| Uitwerking per dienst |
|---|
| **F. Laptops & computers**<br><br>Klant beschikt over een variërend aantal laptops en desktop computers welke door Verwerker zijn ingericht conform de standaard binnen de organisatie. |
| **G. Server/centrale netwerkopslag**<br><br>Algemene kantoordocumenten en overige bestanden van Klant kunnen tevens worden vastgelegd op een lokale eigen server van Klant. Geautoriseerde medewerkers van Klant hebben toegang tot deze bestandsarchieven. |

## 5. Beoogd gebruik

| Uitwerking per dienst |
|---|
| **A. Microsoft Office 365**<br><br>De dienst is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:<br><br>De aard en inhoud van de (persoons)gegevens die Klant vastlegt in een van de onderdelen van Office 365 is bij Verwerker niet bekend.<br><br>Bij deze dienst is rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of door de overheid uitgegeven persoonsnummers.<br><br>Verwerken van deze gegevens met het hiervoor omschreven dienst door Klant is ter eigen beoordeling door Klant. |
| **B. Microsoft Office 365 – Exchange Online**<br><br>De dienst is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:<br><br>De aard en inhoud van de (persoons)gegevens die Klant vastlegt in een van de onderdelen van Office 365 is bij Verwerker niet bekend.<br><br>Bij deze dienst is rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of door de overheid uitgegeven persoonsnummers.<br><br>Verwerken van deze gegevens met het hiervoor omschreven dienst door Klant is ter eigen beoordeling door Klant. |

| Uitwerking per dienst |
| --- |
| **C. Microsoft Office 365 – SharePoint Online & OneDrive voor Bedrijven**<br><br>De dienst is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:<br><br>De aard en inhoud van de (persoons)gegevens die Klant vastlegt in een van de onderdelen van Office 365 is bij Verwerker niet bekend.<br><br>Bij deze dienst is rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of door de overheid uitgegeven persoonsnummers.<br><br>Verwerken van deze gegevens met het hiervoor omschreven dienst door Klant is ter eigen beoordeling door Klant. |
| **D. Backup Online**<br><br>De dienst is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:<br><br>De aard en inhoud van de (persoons)gegevens die Klant vastlegt in een van de onderdelen van Office 365 is bij Verwerker niet bekend.<br><br>Bij deze dienst is rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of door de overheid uitgegeven persoonsnummers.<br><br>Verwerken van deze gegevens met het hiervoor omschreven dienst door Klant is ter eigen beoordeling door Klant. |
| **E. Router, firewall en (draadloos) netwerk**<br><br>De dienst is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:<br><br>Gegevens ter monitoring van het internetverkeer.<br><br>Bij de inrichting van deze dienst is geen rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of door de overheid uitgegeven persoonsnummers. |
| **F. Laptops & computers**<br><br>De dienst is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:<br><br>De aard en inhoud van de (persoons)gegevens die Klant vastlegt in een van de onderdelen van het device is bij Verwerker niet bekend.<br><br>Bij deze dienst is rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of door de overheid uitgegeven persoonsnummers.<br><br>Verwerken van deze gegevens met het hiervoor omschreven dienst door Klant is ter eigen beoordeling door Klant. |

| Uitwerking per dienst |
|---|
| **G. Server/centrale netwerkopslag**<br><br>De dienst is ontworpen en ingericht om er de volgende soort gegevens mee te verwerken:<br><br>De aard en inhoud van de (persoons)gegevens die Klant vastlegt in een van de onderdelen van Office 365 is bij Verwerker niet bekend.<br><br>Bij deze dienst is rekening gehouden met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of door de overheid uitgegeven persoonsnummers.<br><br>Verwerken van deze gegevens met het hiervoor omschreven dienst door Klant is ter eigen beoordeling door Klant. |

## 6. Verwerker heeft bij het ontwerpen van het product/de dienst privacy by design/privacy by default op de volgende wijze toegepast:

| Uitwerking per dienst |
|---|
| **A. Microsoft Office 365**<br><br>• Toegang tot het Office 365 portaal van Klant is voor de gebruikers beveiligd middels een sterk wachtwoord.<br>• De gebruikersaccounts van Klant zijn voorzien van multifactor authenticatie.<br>• Anoniem delen van documenten met externen is beperkt (zie overige Office 365 onderdelen).<br>• Het periodiek wijzigen van wachtwoorden is niet verplicht.<br>• De accounts die gebruikt worden door Verwerker voor beheer, onderhoud en mutaties zijn voorzien van sterke wachtwoorden en multifactor authenticatie. |
| **B. Microsoft Office 365 – Exchange Online**<br><br>Teneinde het 'lekken' van persoonsgegevens tegen te gaan zijn de volgende beleidsregels ingesteld op uitgaande e-mail:<br>• De inhoud van e-mail en bijlagen wordt o.a. gescand op BSN nummers en credit card gegevens. Indien een item dergelijke gegevens bevat, verschijnt er een waarschuwing en krijgt men niet de mogelijkheid om het bericht te versturen.<br>• OPTIE: Gehele tekst mag dan weg.<br>• Er zijn transportregels aangemaakt die er voor zorgen dat e-mail niet automatisch kan worden doorgestuurd naar externe mail adressen (buiten de organisatie).<br>• OPTIE: tekst voor geen blokkade op forwarding e-mails |

| Uitwerking per dienst |
|---|
| **C. Microsoft Office 365 – SharePoint Online & OneDrive voor Bedrijven**<br><br>• Op alle SharePoint onderdelen is het delen van informatie met externe organisaties of personen uitgeschakeld. Uitzonderingen hierop vormen specifiek ingerichte SharePoint sites, waarop externe gebruikers alleen na aanmelding met hun eigen e-mail adres en wachtwoord toegang kunnen krijgen.<br>• Bestanden en mappen welke zijn opgeslagen door gebruikers in OneDrive voor Bedrijven, kunnen met externen worden gedeeld. Ook dit is alleen mogelijk wanneer externen zich kunnen identificeren met hun e-mail adres en een wachtwoord. |
| **D. Backup Online**<br><br>• Backups worden uitsluitend gemaakt op versleutelde bestandslocaties welke niet bereikbaar of toegankelijk zijn voor derden. Voor backups van mailboxen, SharePoint en OneDrive wordt een oplossing van CloudAlly ingezet waarbij de data buiten het Microsoft platform op een redundant datacentrum wordt weggezet. |
| **E. Router, firewall en (draadloos) netwerk**<br><br>• Uitwerking niet van toepassing op deze dienst. |
| **F. Laptops & computers**<br><br>• Laptops en desktop computers welke in gebruik zijn bij Klant, zijn allen voorzien van Bitlocker (voor MAC FileVault) bestandsversleuteling.<br>• Om de kans op gegevensverlies te verkleinen wordt gebruikers geadviseerd om bestanden op de server of in Office 365 bestandslocaties op te slaan (OneDrive en SharePoint). |
| **G. Server/centrale netwerkopslag**<br><br>• Derde partijen (klanten of relaties van Klant) hebben met individueel aangemaakte accounts toegang tot specifiek afgeschermde mappen op de server. Verwerker heeft Klant voorzien van instructies voor het instellen van toegang voor bestaande en nieuwe accounts. Klant draagt zelf zorg voor het genereren van veilige wachtwoorden en verstrekking aan derden. |

**7. Verwerker gebruikt de Standaardclausules voor verwerkingen, welke als bijlage bij de Overeenkomst/Offerte te vinden zijn.**

| Dienst A t/m G - alle diensten |
|---|
| Deze vereiste geldt voor alle diensten. |

**8. Verwerker verwerkt de persoonsgegevens van zijn Klanten binnen de EU/EER.**

| Dienst A t/m G - alle diensten |
|---|
| Deze vereiste geldt voor alle diensten. |

**9. Verwerker maakt gebruik van de volgende subverwerkers:**

| Voor de volgende diensten: | Subverwerker | Binnen of buiten de EU/EER |
|---|---|---|
| A. Microsoft Office 365 | • Microsoft | Binnen EU/EER |
| B. Microsoft Office 365 – Exchange Online | • Microsoft | Binnen EU/EER |
| C. Microsoft Office 365 – SharePoint Online & OneDrive voor Bedrijven | • Microsoft | Binnen EU/EER |
| D. Backup Online | • CloudAlly<br>• AWS (Amazon Web Services | Voor beide subverwerkers: Binnen EU/EER |

**10. Verwerker ondersteunt Klant op de volgende manier bij verzoeken van betrokkenen:**

| Dienst A t/m G - alle diensten |
|---|
| Klant kan zelf gegevens uploaden, inclusief door hen gekozen bijlagen en kan gegevens en bestanden wijzigen en/of verwijderen.<br><br>Verwerker 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. |

**11. Data Pro Statement punt 11 is optioneel en is geen invulling aan gegeven.**

**12. Na beëindiging van de Overeenkomst met een Klant verwijdert Verwerker de persoonsgegevens die hij voor Klant verwerkt in principe binnen 3 maanden op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible).**

| Dienst A t/m G - alle diensten |
| --- |
| Deze vereiste geldt voor alle diensten (A t/m G). |

**13. Na beëindiging van de Overeenkomst met Klant retourneert Verwerker alle persoonsgegevens die hij voor Klant verwerkt binnen 3 maanden op de volgende manier:**

| Dienst A t/m G - alle diensten |
| --- |
| Klant kan vanuit Office 365 zelf een export doen van gegevens. Deze exportmogelijkheid wordt gedurende 2 weken na beëindiging van de Overeengekomen dienstverlening geboden. Daarna worden de gegevens verwijderd.<br><br>De gegevens kunnen op verzoek van Klant via een nader af te stemmen medium worden overgedragen. Vooraf wordt gecommuniceerd of en welke kosten daaraan verbonden zijn. |

## BEVEILIGINGSBELEID

### 14. Verwerker heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn diensten:

**Dienst A t/m G - alle diensten**

Verwerker hanteert het volgende databeveiligingsbeleid:

- Diensten die Verwerker aanbiedt aan Klant zijn enkel afkomstig van gerenommeerde gespecialiseerde leveranciers op het gebied van hun product.
- Verwerker heeft intern duidelijke richtlijnen over het omgaan met vertrouwelijke informatie. Risico's die verbonden zijn aan integriteitsschending worden zoveel mogelijk vermeden.
- Medewerkers tekenen bij indiensttreding een geheimhoudingsverklaring met boeteclausule.
- Persoonsgegevens worden niet gepseudonimiseerd. Verwerker controleert de gegevens van Klant niet en zal gegevens alleen inzien op verzoek van Klant.
- Persoonsgegevens worden wel versleuteld opgeslagen middels encryptie en beveiliging van apparaten zoals laptops, smartphones en opslagmedia.
- De vertrouwelijkheid, integriteit en beschikbaarheid van de oplossingen die worden gebruikt door Klant worden verder als volgt geborgd:
  - Intern huisreglement van Verwerker
  - Certificeringen van subverwerkers
  - Verklaringen en garanties van subverwerkers omtrent beschikbaarheid
  - Maatregelen voor toegangsbeveiliging (multifactor authenticatie, veilige wachtwoorden)
  - Antivirus software op laptops, desktop computers en servers
- Bij incidenten wordt beschikbaarheid van en toegang tot de diensten geborgd door Wachtwoord reset, en/of afdwingen van Multifactor Authenticatie en/of zo nodig door toegang van (gebruikers)accounts pas na verificatie door Klant vrij te geven.

**Beveiligingsmaatregelen per dienst**

**A. Microsoft Office 365**

- Toegang tot het Office 365 portaal van Klant is voor de gebruikers beveiligd middels een sterk wachtwoord.
- De gebruikersaccounts van Klant zijn voorzien van multifactor authenticatie.
- Anoniem delen van documenten met externen is beperkt (zie overige Office 365 onderdelen).
- Het periodiek wijzigen van wachtwoorden is niet verplicht.
- De accounts die gebruikt worden door Verwerker voor beheer, onderhoud en mutaties zijn voorzien van sterke wachtwoorden en multifactor authenticatie.

## Beveiligingsmaatregelen per dienst

### B. Microsoft Office 365 – Exchange Online

Verwerker maakt gebruikersaccounts en mailboxen aan en voert op verzoek van Klant aanpassingen en onderhoud uit, zoals het instellen van toegangsrechten of archiveren van oude gegevens.

- Op mobiele apparaten zoals smartphones en tablets waarop medewerkers e-mail van Klant wensen te synchroniseren, is activatie van een persoonlijke pincode verplicht. Middels de pincode wordt het toestel na 5 minuten inactiviteit automatisch vergrendeld voor gebruik.
- Inkomende e-mail wordt op het Office 365 platform gescand op virussen en malware. Op lokale apparaten zoals werkstations en laptops is de ESET Antivirus software geïnstalleerd, welke middels een zgn. Outlook invoegtoepassing een extra controle doet op ongewenste en mogelijk schadelijke items.
- Bij verlies of diefstal van een mobiel apparaat wordt dit door Klant gemeld bij Verwerker. Verwerker kan evt. op afstand en op aangeven van Klant het betreffende apparaat wissen.
- Op de mailboxen van medewerkers van Klant is Auditing geactiveerd. Hiermee worden mutaties en toegangsdetails van medewerkers, gedelegeerden en beheerders geregistreerd. Vastgelegde details zijn tot 90 dagen terug te raadplegen en op aanvraag te rapporteren door Verwerker.
- Verwijderde e-mails van Klant kunnen standaard tot 30 dagen na datum verwijdering worden hersteld. Mailboxen waarop het zgn. juridische archief is ingeschakeld (Exchange Online Plan 2), daarvan is onbeperkt herstel van e-mail mogelijk.
- Er is een aparte online backup geactiveerd welke dagelijks een volledige kopie van mailbox inhoud maakt buiten het Office 365 platform (zie ook 4. Backup Online).

### C. Microsoft Office 365 – SharePoint Online & OneDrive voor Bedrijven

- Op zowel OneDrive als SharePoint is Auditing geactiveerd. Hiermee worden mutaties en toegangsdetails van medewerkers of externen geregistreerd. Vastgelegde details zijn tot 90 dagen terug te raadplegen en op aanvraag te rapporteren door Verwerker.
- Verwijderde bestanden in SharePoint of OneDrive kunnen standaard tot 90 dagen na datum verwijdering worden hersteld vanuit de prullenbak van de gebruiker of een beheerder.
- Er is een aparte online backup geactiveerd welke dagelijks een volledige kopie van de SharePoint sites maakt buiten het Office 365 platform (zie ook 4. Backup Online).
- Er is een aparte online backup geactiveerd welke dagelijks een volledige kopie van de OneDrive van de gebruikers van Klant maakt buiten het Office 365 platform (zie ook 4. Backup Online).
- OPTIE: Geen backup dan bovenste twee alinea's mogen weg.

### D. Backup Online

- OPTIE: Bij de keuze voor Backup Online, wordt geen additionele backup gemaakt van SharePoint Online, OneDrive en/of Exchange Online.
- Backups van de eigen server worden gemaakt op een beveiligde opslaglocatie binnen het Microsoft Office 365
- Rapportages van de backup worden dagelijks geverifieerd op fouten of problemen. Waar nodig wordt direct actie ondernomen om de correctheid van de backup te borgen.

| Beveiligingsmaatregelen per dienst |
|---|
| **E. Router, firewall en (draadloos) netwerk**<br><br>• De ingebouwde opties van de firewall voor het vastleggen van incidenten en gebeurtenissen zijn ingeschakeld.<br>• De firewall is (niet) voorzien van een abonnement waarmee het internetverkeer op servers, laptops en werkstations gescand wordt op virussen en malware.<br>• Op het internetverkeer van de medewerkers kan (geen) inhoudscontrole en -filtering plaatsvinden.<br>• De firewall van Klant is beveiligd met beheer wachtwoorden welke niet gedeeld zijn met derden.<br>• Het draadloze netwerk omvat een gescheiden gasten gedeelte; het wachtwoord voor toegang tot het eigen/interne netwerk wordt alleen gedeeld met de vaste medewerkers. |
| **F. Laptops & computers**<br><br>• De laptops en desktop computers zijn voorzien van ESET Antivirus. De status hiervan wordt centraal gemonitord door Verwerker. Tevens worden relevante updates voor de software automatisch uitgerold.<br>• OPTIE: De laptops en desktop computers zijn voorzien van antivirus software van Klant, in eigen beheer.<br>• Gebruikers melden zich op de apparaten aan met een zgn. (Azure) Active Directory account. |
| **G. Server/centrale netwerkopslag**<br><br>• De server is voor derden via het internet bereikbaar middels een versleutelde (HTTPS) verbinding op een niet-standaard netwerkpoort.<br>• Bij onjuiste inlogpogingen wordt de verbinding vanaf het bron (IP) adres geblokkeerd gedurende 24 uur.<br>• De logboekregistratie met details omtrent toegang tot de server is geactiveerd.<br>• Dagelijks wordt er een externe (online) backup gemaakt van de bestanden op de server. Hiervoor is een retentietijd ingesteld van 3 maanden.<br>• Het herstellen van bestanden uit de backup wordt -indien nodig- uitgevoerd door Verwerker.<br>• De accounts met beheerderstoegang tot de server zijn beveiligd met multifactor (tweevoudige) authenticatie. |

## 15. Verwerker heeft zich geconformeerd aan het volgende Information Security Management System (ISMS):

- In huis ontwikkelde ISMS versie 1.0 28 april 2020, gebaseerd op de uitgangspunten ISMS Nederland ICT

## 16. Verwerker heeft de volgende certificeringen:

- Data Pro Certificate, gecertificeerd sinds 2020

  * Jaarlijks vindt een hertoetsing plaats
  Per 2023 is de naam Data Pro Certificate veranderd in Data Pro Verified.

## DATALEKPROTOCOL

**17. In geval er toch iets mis gaat, hanteert verwerker het volgende datalekprotocol om ervoor te zorgen dat Klant op de hoogte is van incidenten:**

**Dienst A t/m G - alle diensten**

Verwerker zal zich inspannen de hieronder nader uitgewerkte beveiligingsincidenten te melden aan Klant:

- Besmetting van computers met virussen, malware en/of spyware welke niet hersteld kunnen worden door de geïnstalleerde antivirus software: binnen 4 uur bij de Security Officer van Klant (per e-mail)
- Computers welke niet tijdig voorzien zijn van de automatische beveiligingsupdates van ESET of Microsoft: binnen 3 werkdagen na vaststelling, bij de Security Officer van Klant (per e-mail)

Verwerker heeft in het kader van het melden van beveiligingsincidenten de volgende aanvullende maatregelen getroffen:

- Centrale monitoring van virus incidenten en ongewenste software zoals spyware en malware op computers, met automatische wekelijkse rapportage naar de Security Officer van verwerker.

Verwerker zal bij het doen van zijn melding aan Klant de volgende afspraken in acht nemen:

- Bij doormelding van incidenten worden de volgende details gemeld:
    - Datum en tijdstip van de melding van het incident
    - Aard van het incident

Benodigde vervolgacties ter voorkoming en reparatie van het beveiligingsincident worden besproken met Klant zodra deze contact opneemt met verwerker.

De Security Officer (of het aanspreekpunt) van Klant is primair contactpersoon voor genoemde incidenten.

Kosten die gemaakt worden in het kader van de melding van een beveiligingsincident, en het nemen van aanvullende maatregelen ter voorkoming van een nieuw incident, worden doorberekend aan Klant op basis van de daadwerkelijk besteedde tijd en door verwerker gemaakte kosten.