PROLOCATION	Verklaring van compliance met NIS2/DORA	
	Datum: 09-12-2025	Versie: 1.0
	Eigenaar: Christiaan den Besten	Pagina 1 van 1

Inhoud

Doel van dit document

Bedrijven en organisaties die rechtstreeks onder het Nederlandse NIS2-regime vallen, moeten naar de veiligheid van hun keten kijken. Als toeleverancier van NIS2-bedrijven of -organisaties krijgt Prolocation mogelijk indirect met de regelgeving en daaruit voortvloeiende vragen te maken. Om proactief helderheid te verschaffen in de wijze waarop Prolocation als toeleverancier informatiebeveiliging (en kwaliteit) heeft geborgd, is dit document opgesteld. De NIS2-richtlijn moet nog worden overgezet naar de Nederlandse wetgeving: de Cyberbeveiligingswet (Cbw / NIS2) en de Wet weerbaarheid kritieke entiteiten (Wwke/CER)3. Naar verwachting treden de nieuwe wetten in vanaf het tweede kwartaal van 2026, derhalve vindt de mapping plaatst op de NIS2 uitgangspunten zelf.

Het Informatiebeveiligingsbeleid van Prolocation

Voorwoord directie

Dit document beschrijft het beleid van Prolocation met betrekking tot de beveiliging van informatie. De informatievoorziening is van essentieel belang voor de continuïteit van de bedrijfsvoering van de organisatie en haar klanten. Zowel op papier als geautomatiseerd zijn wij en onze klanten bij ons dagelijks werk afhankelijk van de beschikbaarheid van betrouwbare informatie. Onze organisatie en informatievoorziening worden blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard. Deze dreigingen maken het noodzakelijk om gerichte maatregelen te treffen om risico's tot een aanvaardbaar niveau te reduceren. Het proces van informatiebeveiliging begint met het definiëren van een beleid op dit punt. Het beleid is vastgelegd in dit document en door de directie vastgesteld.

Doel

Ten behoeve van de privacy- en informatiebeveiliging zijn een reeks beleidsregels gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en beschikbaar gesteld en op aanvraag aan relevante externe partijen.

Reikwijdte van dit beleid

Dit beleid is van toepassing op alle informatie die gecreëerd, ontvangen, verzonden of bewaard wordt in de dienstverlening van Prolocation aan klanten en de daarmee samenhangende wettelijke, contractuele verplichtingen en ondersteunende processen. Het beleid en de uitwerking hiervan gelden voor alle medewerkers van Prolocation. Afwijkingen hierop moeten gemeld worden, zodat het managementsysteem continu verbeterd wordt. Daarnaast geldt het beleid ook voor contractanten, die Prolocation ondersteunen bij haar dienstverlening aan klanten.

Onlosmakelijk onderdeel van dit beleid zijn interne gedragsregels waaraan ook alle medewerkers, contractanten en stagiaires zich moeten houden. Er wordt zoveel mogelijk gestreefd naar beveiligingsmaatregelen die gebaseerd zijn op logische principes, omdat deze kosteneffectief en duurzaam zijn. Deze principes zijn:

- Vertrouwelijke gegevens die je niet hebt, hoef je ook niet te beveiligen.
- Niet slepen met vertrouwelijke gegevens.
- Scheiden van gegevens.

Prolocation werkt conform ISO 27001 en is daarmee uiteindelijk verantwoordelijk voor het veilig beschikbaar stellen van haar diensten. Prolocation stelt haar klanten daarmee in staat om veilig de diensten van Prolocation te gebruiken. Dit ontslaat echter de klant niet van de eindverantwoordelijkheid voor de beveiliging van haar eigen informatievoorziening.

Pijlers onder het beleid

Optimale beheersing

Prolocation streeft naar een optimale beheersing van informatiebeveiligingsrisico's. Optimaal betekent voor Prolocation een acceptabel risiconiveau tegen aanvaardbare kosten. Beheersmaatregelen worden genomen op basis van een risicobeoordeling. Wij actualiseren ons risicobeeld minimaal jaarlijks.

Bewustwording

Prolocation beseft zich dat verhogen van de bewustwording t.a.v. informatiebeveiliging essentieel is in deze context en dat niet alleen kan worden vertrouwd op beschreven procedures. Het gehele management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt.

Commitment

De medewerkers van Prolocation - zowel vast als tijdelijk, intern of extern - hebben zich gecommitteerd aan ons informatiebeveiligingsbeleid en onze gedragsregels. Alle medewerkers van Prolocation worden getraind in het gebruik van beveiligingsprocedures.

Betrouwbare partners

Prolocation werkt samen met betrouwbare partners. Waar noodzakelijk en mogelijk stellen wij eisen t.a.v. informatiebeveiliging aan onze partners. Wij monitoren dat onze vertrouwelijke gegevens bij partners in veilige handen zijn.

Compliance

Het informatiebeveiligingsbeleid van Prolocation is in lijn met de relevante landelijke en Europese wet- en regelgeving. Het beleid wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, geregistreerde incidenten en risicoanalyses.

Beleidsuitgangspunten

Met onderstaande kwalitatieve beleidsuitgangspunten verwacht Prolocation haar informatiebeveiligingsrisico's te beheersen en tegelijk haar flexibiliteit en efficiëntie bij het uitvoeren van haar werkzaamheden te behouden. De beleidsuitgangspunten vormen de brug tussen de informatiebeveiligingsrisico's en de beheersdoelstellingen en -maatregelen. De beleidsuitgangspunten bieden bovendien het kader voor de directie, op welke wijze zij wil dat de informatiebeveiligingsdoelstellingen worden vormgegeven, die passend zijn voor Prolocation.

Bij de verdere invulling van dit beleid gelden de volgende uitgangspunten:

1. Informatiebeveiliging is een belangrijk bedrijfsrisico voor Prolocation. De directie stelt daarom het beleid vast, beoordeelt de risico's, stelt de maatregelen vast, stelt voldoende middelen ter beschikking en laat periodiek de werking van het beleid en de naleving van deze maatregelen intern en extern beoordelen om te borgen, dat het IB-managementsysteem blijvend adequaat werkt en waar nodig verbeterd wordt.
2. Prolocation conformeert zich m.b.t. de informatiebeveiliging aan de relevante wetgeving en de contractuele afspraken met klanten en business partners.
3. Prolocation streeft ernaar om haar dienstverlening aan klanten continu te verbeteren.
4. De beheersdoelstellingen en beheersmaatregelen van de norm NEN-ISO/IEC 27001 en de privacyrichtlijnen van de Autoriteit Persoonsgegevens (AP) vormen, voor zover zij bijdragen aan de informatiebeveiliging van Prolocation en handhaafbaar zijn, het uitgangspunt voor de te definiëren maatregelen. Dit is vooral een bedrijfseconomische afweging.
5. Prolocation beschouwt computercriminaliteit als een ongewenst maatschappelijk probleem en ziet het slechts als haar taak om passende maatregelen te nemen om schade ten gevolge van criminele activiteiten zoveel mogelijk te beperken.
6. Vertrouwen is voor Prolocation een groot goed en zij hanteert naar medewerkers, klanten, leveranciers en andere stakeholders het wederkerigheidsprincipe. Prolocation gaat ervan uit, dat zij afspraken nakomen m.b.t. beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening.
7. Het HRM-beleid is mede gericht op het verbeteren van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening bij medewerkers. Tijdens een jaarlijkse evaluatie wordt dit aan de orde gesteld. Beleidspunten voor informatiebeveiliging zijn voor onze medewerkers vertaald naar een praktische gedragscode.

8. De fysieke en logistieke beveiliging van de gebouwen en de ruimtes daarin zijn zodanig, dat de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens en gegevensverwerking inclusief de bedrijfsmiddelen gewaarborgd zijn.
9. Ontwikkeling of aanschaf, installatie en onderhoud van informatie- en communicatiesystemen, alsmede inpassing van nieuwe technologieën, moeten zo nodig met aanvullende maatregelen worden uitgevoerd, dat hiermee geen afbreuk wordt gedaan aan de informatiebeveiliging.
10. Opdrachten aan derden voor het uitvoeren van werkzaamheden worden zodanig omgeven met maatregelen, dat er geen inbreuk op de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening kan ontstaan.
11. Bij de verwerking en het gebruik van gegevens worden maatregelen getroffen om de privacy van klanten, medewerkers en andere betrokkenen te waarborgen. We hanteren een ‘clear desk’-beleid voor papier en verwijderbare opslagmedia en een ‘clear screen’-beleid voor IT-voorzieningen. Voor het gebruik van ‘User endpoint devices’ zijn afspraken gemaakt.
12. Toegangsbeveiliging zorgt ervoor, dat ongeautoriseerde personen of processen geen toegang krijgen tot de informatiesystemen, gegevensbestanden en programmatuur van Prolocation. Ten aanzien van het gebruik van netwerkdiensten is ons uitgangspunt dat gebruikers alleen toegang wordt verleend tot diensten waarvoor ze specifiek bevoegd zijn.
13. Gegevensverstrekking extern gebeurt op basis van 'need to know'. Intern is dit niet altijd wenselijk omdat kennisdeling essentieel is voor een kosteneffectieve dienstverlening aan klanten.
14. Prolocation en haar medewerkers treffen maatregelen om te voorkomen, dat vertrouwelijke informatie in handen van derden terechtkomt.
15. Input van klanten die vertrouwelijke data bevat, wordt na verwerking op korte termijn gearchiveerd of vernietigd.
16. Datatransport is zodanig met beveiligingsmaatregelen omkleed, dat geen inbreuk kan worden gepleegd op de vertrouwelijkheid en de integriteit van deze gegevens.
17. Geautoriseerde medewerkers moeten ook op afstand een beveiligde toegang hebben tot de voor hun relevante productieomgevingen. Er worden geen vertrouwelijke gegevens buiten de productieomgeving opgeslagen. Onder condities kan hiervan afgeweken worden. We hanteren een strikt thuiswerkbeleid.
18. Productieomgevingen zijn gescheiden van andere omgevingen en hierin kunnen specifiek toegangsrechten worden verleend en is monitoring van de toegang mogelijk.

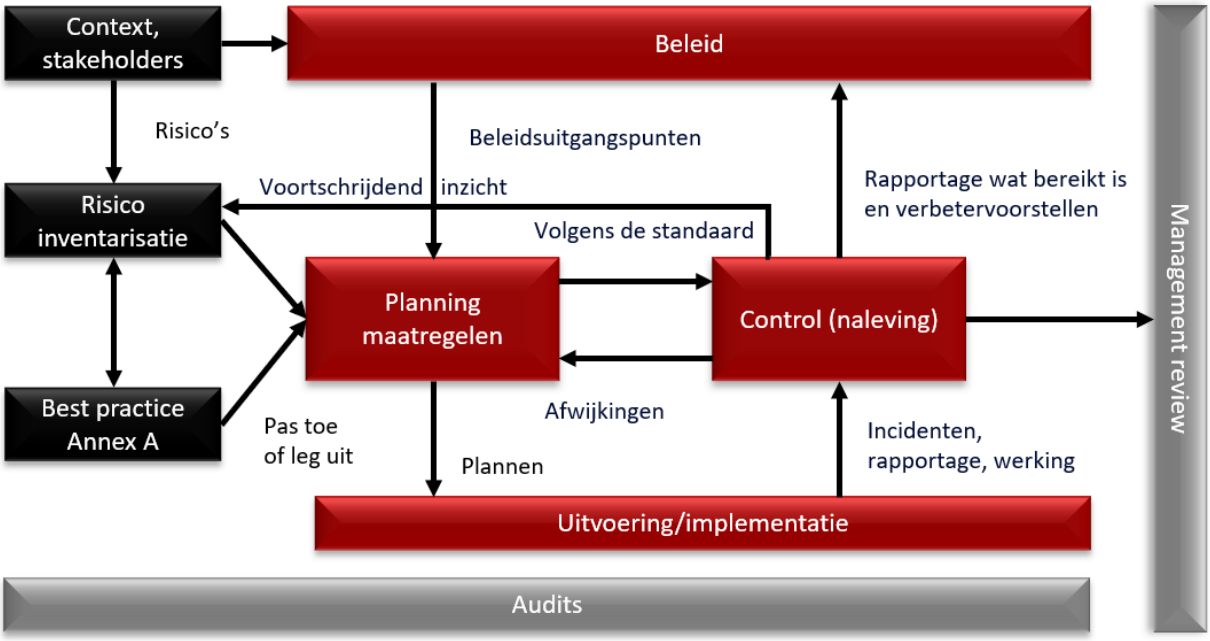
19. Het beheer en de opslag van gegevens in productieomgevingen zijn zodanig, dat geen informatie verloren kan gaan tenzij er sprake is van overmacht.
20. Er zijn functiescheidingen aangebracht tussen de ontwikkel-, beheer- en gebruikersorganisatie. Verder wordt functiescheiding toegepast waar dat mogelijk en wenselijk is.
21. Er is beleid op het gebied van cryptografische beheersmaatregelen voor de bescherming van informatie. Dit is met name van belang bij informatie-uitwisseling met klanten met een hoog informatiebeveiligingsprofiel.
22. Er is een proces om incidenten adequaat af te handelen en hier 'lessons learned' uit te trekken.
23. Er zijn calamiteitenplannen en -voorzieningen om de beschikbaarheid van de informatievoorziening te waarborgen. We werken met een business continuïteitsplan waarin informatiebeveiliging een belangrijke plaats inneemt.
24. Bij uitbesteding van gegevensverwerking kan de directie besluiten om tijdelijk af te wijken van deze beleidsuitgangspunten en de risico's hiervan tijdelijk te accepteren.
25. Opdrachten aan derden voor het uitvoeren van werkzaamheden worden zodanig omgeven met maatregelen, dat er geen inbreuk op de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening kan ontstaan.
26. Bij conflicten prevaleert de missie van Prolocation boven de eisen die gesteld worden door IB en of privacy.
27. Informatiebeveiliging is onderdeel van het ontwerpen, ontwikkelen en beheren van software, ook als die door derden wordt ontwikkeld. Security by design en privacy by design en default vormen hierbij de voornaamste uitgangspunten.
28. Prolocation en haar medewerkers realiseren zich de privacy gevoeligheid van de (bijzondere) persoonsgegevens die zij verwerken en waarborgen te allen tijde de afscherming, corrigeerbaarheid en transparantie van deze gegevens ter bescherming van de persoonlijke levenssfeer van de betrokkenen.

Het Information Security Management System (ISMS)

Dit beleid is uitgewerkt in een Information Security Management System (ISMS) waarin de belangrijkste procedures en andere informatie zijn vastgelegd. Het ISMS is van toepassing op de gehele organisatie, alle processen, informatiesystemen en gegevens(verzamelingen), waarvoor Prolocation (risico)verantwoordelijk is.

Op basis van dit beleid worden risicoanalyses uitgevoerd en wordt een set van maatregelen van toepassing verklaard en geïmplementeerd, al dan niet aangevuld met eigen maatregelen om het risico verder te beperken. In de Verklaring van Toepasselijkheid is vastgelegd welke elementen van de ISO 27001 (Annex A) zijn opgenomen dan wel uitgesloten.

Het ISMS moet borgen dat Prolocation blijvend voldoet aan relevante informatiebeveiligingseisen, zoals volgt uit de ISO27001 norm en relevante wet- en regelgeving. Informatiebeveiliging is een continu verbeterproces. Het ISMS kent een 'Plan, do, check en act' cyclus, waardoor continue verbetering en bijsturing mogelijk zijn:



Controle werking en naleving van het beleid

In de directiebeoordeling wordt de werking en de naleving van het beleid intern geëvalueerd en zo nodig aangepast. Jaarlijks wordt een interne audit gehouden. Onderdeel van de interne auditrapportage zijn afwijkingen en suggesties ter verbetering. De directie beoordeelt de rapportage, keurt voorstellen al dan niet goed en kent budget toe voor de realisatie van de voorstellen.

Daarnaast wordt jaarlijks een externe audit uitgevoerd op de werking van het managementsysteem door een onafhankelijke derde partij, die hiertoe bevoegd en deskundig is.

Interne en externe publicatie

Dit beleid is gecommuniceerd aan alle medewerkers (internen, externen). Op verzoek is dit beleid beschikbaar voor belanghebbende derden.

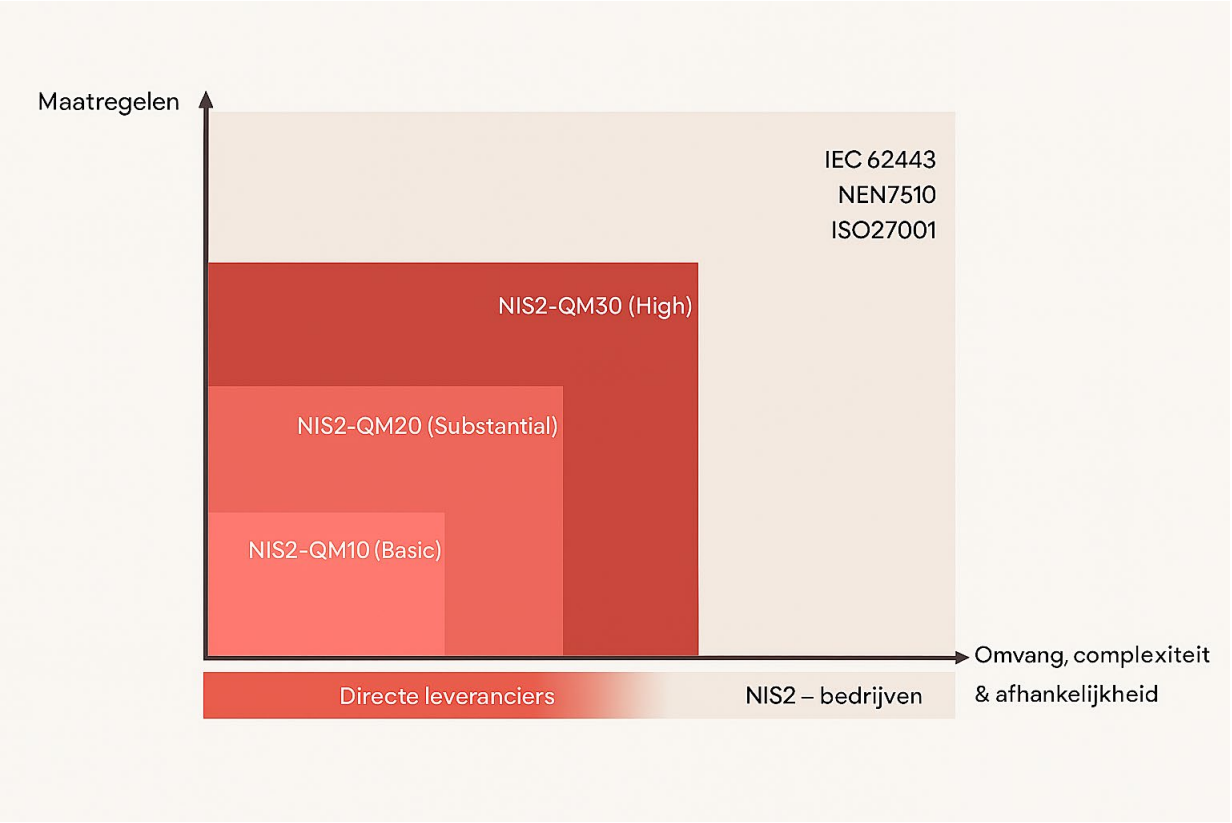
Datum

Handtekening

Hoe zorgt de ISO-27001 certificering voor een goede borging

Het informatiebeveiligingsmanagement systeem (ISMS) van Prolocation is gebaseerd op de internationale standaard voor informatiebeveiliging ISO-27001:2022 inclusief NEN-7510:2024 (zorgspecifieke maatregelen waar toepasselijk).

Er wordt ook veel gesproken over Quality Mark als een toetsing voor informatiebeveiliging. De ISO-27001 en NEN-7510 standaard zijn breder op dit vlak.



De norm valt uiteen in 2 onderdelen, de norm zelf (zie hieronder de referenties naar paragrafen) en een reeks maatregelen (zie hieronder de referenties naar Annex A maatregelen), samengesteld uit best practises uit ISO-27001/ ISO-27002 en geïmplementeerde eigen maatregelen. Het gaat hier om

maatregelen die relevant kunnen zijn om risico's ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid van informatie te beheersen, te vermijden of te reduceren.

Er is een duidelijke overeenkomst in de uitgangspunten uit de NIS2 (en daarmee uiteindelijke ook de Cyberbeveiligingswet) en de ISO-27001 standaard.

Article 21: Cyber security risk management measures	**ISO-27001**	**Onderwerp**
(A) Policies on risk analysis and information system security	§5.2	Informatiebeveiligingsbeleid
	§6.1.2	Informatiebeveiliging risicobeoordelingsproces
	§6.1.3	Informatiebeveiliging risicobehandelingsproces
	§8.2	Informatiebeveiliging risicobeoordeling
	§8.3	Informatiebeveiliging risicobeoordeling
(F) Policies and procedures to assess the effectiveness of cybersecurity risk management measures	§9.1	Monitoren, meten, analyseren en evalueren
	§9.2	Interne audit
	§9.3	Management review
G) Basic cyber hygiene practices and cybersecurity training;	§7.3	Bewustzijn
	§7.4	Communicatie

PROLOCATION	Verklaring van compliance met NIS2/DORA	
	Datum: 09-12-2025	Versie: 1.0
	Eigenaar: Christiaan den Besten	Pagina 1 van 1

De Verklaring van Toepasselijkheid van Prolocation en NIS2/DORA relatie

Via het onderstaande overzicht gebaseerd op de Verklaring van Toepasselijkheid van Prolocation vs 2.0 09/09/2025 van wordt inzicht geboden in de mate waarin best practices uit de ISO-27001 normering zijn geïmplementeerd door Prolocation en zijn ingezet om risico's af te dekken. In de laatste kolom is aangegeven hoe dit parallel loopt met de eisen uit NIS2 voor NIS2- entiteiten.

ID	Omschrijving	Naam beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag (Reden van insluiting)	NIS2/DORA relatie
5	**Organisatorische beheersmaatregelen**					
5.1	Beleidsregels voor informatiebeveiliging	Informatiebeveiligingsbeleid en onderwerpspecifieke beleidsregels moeten worden gedefinieerd, goedgekeurd door het management, gepubliceerd, gecommuniceerd aan en erkend door relevant personeel en relevante belanghebbenden en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, worden beoordeeld.	Ja		☑ RB ☑ WG ☑ CV	Article 20: Governance Article 21: Cyber security risk management measures: (A) Policies on risk analysis and information system security
5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen	Ja		☑ RB ☐ WG ☐ CV	

ID	Omschrijving	Naam beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag (Reden van insluiting)	NIS2/DORA relatie
		overeenkomstig de behoeften van de organisatie				
5.3	Functiescheiding	Conflicterende taken en conflicterende verantwoordelijkheden moeten worden gescheiden.	Ja		☑ RB ☐ WG ☐ CV	
5.4	Management-verantwoordelijkheden	Het management moet van al het personeel eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de onderwerpspecifieke beleidsregels en procedures van de organisatie.	Ja		☑ RB ☐ WG ☐ CV	
5.5	Contact met overheidsinstanties	De organisatie moet contact met de relevante instanties leggen en onderhouden.	Ja		☑ RB ☐ WG ☐ CV	
5.6	Contact met speciale belangengroepen	De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en onderhouden.	Ja		☑ RB ☐ WG ☐ CV	
5.7	Informatie en analyses over dreigingen	Informatie met betrekking tot informatiebeveiligingsdreigingen moet worden verzameld en geanalyseerd om informatie en analyses over dreigingen te produceren.	Ja		☑ RB ☐ WG ☐ CV	
5.8	Informatiebeveiliging in projectmanagement	Informatiebeveiliging moet worden geïntegreerd in projectmanagement.	Ja		☑ RB ☐ WG ☐ CV	
5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Er moet een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, worden opgesteld en onderhouden.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: I) Human resources security, access control policies and asset management

ID	Omschrijving	Naam beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag (Reden van insluiting)	NIS2/DORA relatie
ZORG	Zorgspecifieke beheersmaatregel (aanvullend)		Nee	Valt onder de verantwoordelijkheid van de klant voor zover van toepassing.		
5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen moeten worden vastgesteld, gedocumenteerd en geïmplementeerd.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: I) Human resources security, access control policies and asset management
5.11	Retourneren van bedrijfsmiddelen	Personeel en andere belanghebbenden, al naargelang de situatie, moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst retourneren.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: I) Human resources security, access control policies and asset management
ZORG	Zorgspecifieke beheersmaatregel (aanvullend)		Ja		idem	
5.12	Classificeren van informatie	Informatie moet worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante belanghebbenden.	Ja		☑ RB ☐ WG ☐ CV	
ZORG	Zorgspecifieke beheersmaatregel (aanvullend)		Ja		☑ idem	
5.13	Labelen van informatie	Om informatie te labelen moet een passende reeks procedures worden vastgesteld en geïmplementeerd in overeenstemming met het	Ja		☑ RB ☐ WG ☐ CV	

ID	Omschrijving	Naam beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag (Reden van insluiting)	NIS2/DORA relatie
		informatieclassificatieschema dat is vastgesteld door de organisatie.				
5.14	Overdragen van informatie	Er moeten regels, procedures of overeenkomsten voor informatieoverdracht zijn vastgesteld voor alle soorten van overdracht binnen de organisatie en tussen de organisatie en andere partijen.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (J) Use of MFA or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate. Article 23 Reporting obligations
ZORG	Zorgspecifieke beheersmaatregel (aanvullend)		Ja		☑ idem	
5.15	Toegangsbeveiliging	Er moeten regels op basis van bedrijfs- en informatiebeveiligingseisen worden vastgesteld en geïmplementeerd om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: G) Basic cyber hygiene practices and cybersecurity training. I) Human resources security, access control policies and asset management
ZORG	Zorgspecifieke beheersmaatregel (aanvullend)		Ja		☑ idem	
5.16	Identiteitsbeheer	De volledige levenscyclus van identiteiten moet worden beheerd.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: G) Basic cyber hygiene practices and cybersecurity training I) Human resources security, access control policies and asset management (J) Use of MFA or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.
ZORG	Zorgspecifieke beheersmaatregel (aanvullend)		Ja		☑ idem	
5.17	Beheren van authenticatie-informatie	De toewijzing en het beheer van authenticatie-informatie moet worden	Ja		☑ RB ☐ WG	Article 21: Cyber security risk management measures: I) Human resources security,

ID	Omschrijving	Naam beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag (Reden van insluiting)	NIS2/DORA relatie
		beheerst door middel van een beheerproces waarvan het informeren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.			☐ CV	access control policies and asset management (J) Use of MFA or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.
5.18	Toegangsrechten	Toegangsrechten met betrekking tot informatie en andere gerelateerde bedrijfsmiddelen moeten worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de organisatie.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: G) Basic cyber hygiene practices and cybersecurity training I) Human resources security, access control policies and asset management
5.19	Informatiebeveiliging in leveranciersrelaties	Er moeten processen en procedures worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met het gebruik van producten of diensten van de leverancier te beheren.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (D) Supply chain security including security related aspects concerning the relationships between eacht entity and its direct suppliers or service providers
ZORG	Zorgspecifieke beheersmaatregel (aanvullend)		Ja		☑ idem	
5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Relevante informatiebeveiligingseisen moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie worden overeengekomen.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (D) Supply chain security including security related aspects concerning the relationships between each entity and its direct suppliers or service providers (E) Security in network and information systems acquisitions, development and maintenance including vulnerability handling and disclosure

ID	Omschrijving	Naam beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag (Reden van insluiting)	NIS2/DORA relatie
						Article 24 Use of European cybersecurity certification schemes
5.21	Beheren van informatiebeveiliging in de ICT-keten	Er moeten processen en procedures worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheren.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (D) Supply chain security including security related aspects concerning the relationships between each entity and its direct suppliers or service providers
5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	De organisatie moet de informatiebeveiligingspraktijken en de leveranciersdiensten regelmatig monitoren, beoordelen, evalueren en veranderingen daaraan beheren.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (D) Supply chain security including security related aspects concerning the relationships between each entity and its direct suppliers or service providers
5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten moeten overeenkomstig de informatiebeveiligingseisen van de organisatie worden opgesteld.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (D) Supply chain security including security related aspects concerning the relationships between each entity and its direct suppliers or service providers
5.24	Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	De organisatie moet plannen op stellen voor, en zich voorbereiden op, het beheren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (B) Incident handling (E) Security in network and information systems acquisitions, development and maintenance including vulnerability handling and disclosure G) Basic cyber hygiene practices and cybersecurity training;
5.25	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (B) Incident handling

ID	Omschrijving	Naam beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag (Reden van insluiting)	NIS2/DORA relatie
5.26	Reageren op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (B) Incident handling
5.27	Leren van informatiebeveiligingsincidenten	Kennis die is opgedaan met informatiebeveiligingsincidenten moet worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (B) Incident handling
5.28	Verzamelen van bewijsmateriaal	De organisatie moet procedures vaststellen en implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (B) Incident handling
5.29	Informatiebeveiliging tijdens een verstoring	De organisatie moet plannen maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (C) Business Continuity, such as backup management and disaster recovery and crisis management
5.30	ICT-gereedheid voor bedrijfscontinuïteit	De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (C) Business Continuity, such as backup management and disaster recovery and crisis management
5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Eisen van wettelijke, statutaire, regelgevende en contractuele eisen die relevant zijn voor informatiebeveiliging en de aanpak van de organisatie om aan deze eisen te voldoen moeten worden vastgesteld, gedocumenteerd en actueel gehouden.	Ja		☑ RB ☑ WG ☐ CV	Article 20: Governance
5.32	Intellectuele eigendomsrechten	De organisatie moet passende procedures implementeren om	Ja		☑ RB ☑ WG	

ID	Omschrijving	Naam beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag (Reden van insluiting)	NIS2/DORA relatie
		intellectuele eigendomsrechten te beschermen.			☑ CV	
5.33	Beschermen van registraties	Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	Ja		☑ RB ☑ WG ☐ CV	
5.34	Privacy en bescherming van persoonsgegevens	De organisatie moet de eisen met betrekking tot het behoud van privacy en de bescherming van persoonsgegevens volgens de toepasselijke wet- en regelgeving en contractuele eisen identificeren en eraan voldoen.	Ja		☑ RB ☑ WG ☐ CV	Article 20: Governance
5.35	Onafhankelijke beoordeling van informatiebeveiliging	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan, met inbegrip van mensen, processen en technologieën, moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, worden beoordeeld.	Ja		☑ RB ☐ WG ☐ CV	Article 20: Governance Article 21: Cyber security risk management measures: (F) Policies and procedures to assess the effectiveness of cybersecurity risk management measures
5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie moet regelmatig worden beoordeeld.	Ja		☑ RB ☐ WG ☐ CV	Article 20: Governance Article 21: Cyber security risk management measures: (F) Policies and procedures to assess the effectiveness of cybersecurity risk management measures
5.37	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar te worden gesteld aan het personeel dat ze nodig heeft.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (E) Security in network and information systems acquisitions, development and maintenance including vulnerability handling and disclosure

ID	Omschrijving	Naam beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag (Reden van insluiting)	NIS2/DORA relatie
5.38	HLT – Analyse en specificatie van informatiebeveiligingseisen	Zorgspecifieke beheersmaatregel	Nee	Geen, n.v.t. gezondheidssystemen in beheer of eigendom		
5.39	HLT – Zorgontvangers op unieke wijze identificeren	Zorgspecifieke beheersmaatregel	Nee	De relatie met de zorgontvangers is aan de klantzijde geborgd. Prolocation is geen verwerkingsverantwoordelijke.		
5.40	HLT – Validatie van getoonde/geprinte gegevens	Zorgspecifieke beheersmaatregel	Nee	Prolocation levert geen gezondheidsinformatiesystemen.		
5.41	HLT – Openbaar beschikbare gezondheidsinformatie	Zorgspecifieke beheersmaatregel	Nee	De organisatie creëert geen openbaar beschikbare gezondheidsinformatie.		
5.42	HLT – Communicatie in noodsituaties	Zorgspecifieke beheersmaatregel	Nee	De organisatie beheert geen noodcommunicatiekanalen binnen een zorgorganisatie		
5.43	HLT – Incidenten extern melden	Zorgspecifieke beheersmaatregel	Ja		☑ RB ☐ WG ☐ CV	

ID	Omschrijving	Naam beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag (Reden van insluiting)	NIS2/DORA relatie
6	**Mensgerichte beheersmaatregelen**					
6.1	Screening	De achtergrond van alle kandidaten die in aanmerking komen voor posities binnen de organisatie moet worden gecontroleerd voordat ze bij de organisatie in dienst treden en daarna op gezette tijden worden herhaald. Hierbij moet rekening worden gehouden met de toepasselijke wet- en regelgeving, voorschriften en ethische overwegingen, en deze controle moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: I) Human resources security, access control policies and asset management
6.2	Arbeidsovereenkomst	In arbeidsovereenkomsten behoort te worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: I) Human resources security, access control policies and asset management
ZORG	Zorgspecifieke beheersmaatregel (aanvullend)		Ja		Idem	
6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Personeel van de organisatie en relevante belanghebbenden behoren een passend(e) bewustwording van, opleiding, training en bijscholing in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en procedures van de organisatie, voor	Ja		☑ RB ☐ WG ☐ CV	Article 20: Governance Article 21: Cyber security risk management measures: G) Basic cyber hygiene practices and cybersecurity training;

ID	Omschrijving	Naam beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag (Reden van insluiting)	NIS2/DORA relatie
		zover relevant voor hun functie, te krijgen.				
6.4	Disciplinaire procedure	Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen personeel en andere belanghebbenden die zich schuldig hebben gemaakt aan een schending van het informatiebeveiligingsbeleid.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: I) Human resources security, access control policies and asset management
6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband behoren te worden gedefinieerd, gehandhaafd en gecommuniceerd aan relevant personeel en andere belanghebbenden.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: G) Basic cyber hygiene practices and cybersecurity training I) Human resources security, access control policies and asset management
6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, behoren te worden geïdentificeerd, gedocumenteerd, regelmatig te worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: I) Human resources security, access control policies and asset management
ZORG	Zorgspecifieke beheersmaatregel (aanvullend)		Ja		Idem	
6.7	Werken op afstand	Wanneer personeel op afstand werkt, behoren er beveiligingsmaatregelen te worden geïmplementeerd om informatie te beschermen die buiten het gebouw en/of terrein van de organisatie wordt ingezien, verwerkt of opgeslagen.	Ja		☑ RB ☐ WG ☐ CV	

ID	Omschrijving	Naam beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag (Reden van insluiting)	NIS2/DORA relatie
6.8	Melden van informatiebeveiligingsgebeurtenissen	De organisatie behoort te voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (B) Incident handling (E) Security in network and information systems acquisitions, development and maintenance including vulnerability handling and disclosure G) Basic cyber hygiene practices and cybersecurity training Article 23 Reporting obligations
6.9	HLT – Managementtraining	Zorgspecifieke beheersmaatregel	Ja		☑ RB ☐ WG ☐ CV	
7	**Fysieke beheersmaatregelen**					
7.1	Fysieke beveiligingszones	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken.	Ja		☑ RB ☐ WG ☐ CV	
7.2	Fysieke toegangsbeveiliging	Beveiligde zones moeten worden beschermd door passende toegangscontroles en toegangspunten.	Ja		☑ RB ☐ WG ☐ CV	
7.3	Beveiligen van kantoren, ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.	Ja		☑ RB ☐ WG ☐ CV	
7.4	Monitoren van de fysieke beveiliging	Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.	Ja		☑ RB ☐ WG ☐ CV	
7.5	Beschermen tegen fysieke en omgevingsdreigingen	Er moet bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen van de infrastructuur, worden ontworpen en geïmplementeerd.	Ja		☑ RB ☐ WG ☐ CV	

ID	Omschrijving	Naam beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag (Reden van insluiting)	NIS2/DORA relatie
7.6	Werken in beveiligde zones	Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd.	Ja		☑ RB ☐ WG ☐ CV	
7.7	'Clear desk' en 'clear screen'	Er moeten 'clear desk'-regels voor papieren documenten en verwijderbare opslagmedia en 'clear screen'-regels voor informatieverwerkende faciliteiten worden gedefinieerd en op passende wijze ten uitvoer worden gebracht.	Ja		☑ RB ☐ WG ☐ CV	
7.8	Plaatsen en beschermen van apparatuur	Apparatuur moet veilig worden geplaatst en beschermd.	Ja		☑ RB ☐ WG ☐ CV	
7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd.	Ja		☑ RB ☐ WG ☐ CV	
7.10	Opslagmedia	Opslagmedia moeten worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie.	Ja		☑ RB ☐ WG ☐ CV	
ZORG	Zorgspecifieke beheersmaatregel (aanvullend)		Ja		idem	
7.11	Nutsvoorzieningen	Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	Ja		☑ RB ☐ WG ☐ CV	
7.12	Beveiligen van bekabeling	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen	Ja		☑ RB ☐ WG ☐ CV	

ID	Omschrijving	Naam beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag (Reden van insluiting)	NIS2/DORA relatie
		onderschepping, interferentie of beschadiging.				
7.13	Onderhoud van apparatuur	Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.	Ja		☑ RB ☐ WG ☐ CV	
7.14	Veilig verwijderen of hergebruiken van apparatuur	Onderdelen van de apparatuur die opslagmedia bevatten, moeten worden gecontroleerd om te waarborgen dat gevoelige gegevens en gelicentieerde software zijn verwijderd of veilig zijn overschreven voordat ze worden verwijderd of hergebruikt.	Ja		☑ RB ☐ WG ☐ CV	
8	**Technologische beheersmaatregelen**				☑	
8.1	'User endpoint devices'	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' moet worden beschermd.	Ja		☑ RB ☐ WG ☐ CV	
8.2	Speciale toegangsrechten	Het toewijzen en gebruik van speciale toegangsrechten moeten worden beperkt en beheerd.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: G) Basic cyber hygiene practices and cybersecurity training;
8.3	Beperking toegang tot informatie	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen moet worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: G) Basic cyber hygiene practices and cybersecurity training;
8.4	Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd.	Ja		☑ RB ☐ WG ☐ CV	

ID	Omschrijving	Naam beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag (Reden van insluiting)	NIS2/DORA relatie
8.5	Beveiligde authenticatie	Er moeten beveiligde authenticatietechnologieën en -procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke of aanvullende beleid inzake toegangsbeveiliging.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: G) Basic cyber hygiene practices and cybersecurity training;
ZORG	Zorgspecifieke beheersmaatregel (aanvullend)		Ja		idem	
8.6	Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en afgestemd overeenkomstig de huidige en verwachte capaciteitseisen.	Ja		☑ RB ☐ WG ☐ CV	
8.7	Bescherming tegen malware	Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: G) Basic cyber hygiene practices and cybersecurity training;
8.8	Beheer van technische kwetsbaarheden	Er moet informatie worden verkregen over technische kwetsbaarheden van in gebruik zijnde informatiesystemen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en er moetende passende maatregelen worden getroffen.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (E) Security in network and information system acquisitions, development and maintenance including vulnerability handling and disclosure
8.9	Configuratiebeheer	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (E) Security in network and information system acquisitions, development and maintenance including vulnerability handling and disclosure G) Basic cyber hygiene practices and cybersecurity training;
8.10	Wissen van informatie	In informatiesystemen, apparaten of andere opslagmedia opgeslagen	Ja		☑ RB ☑ WG	

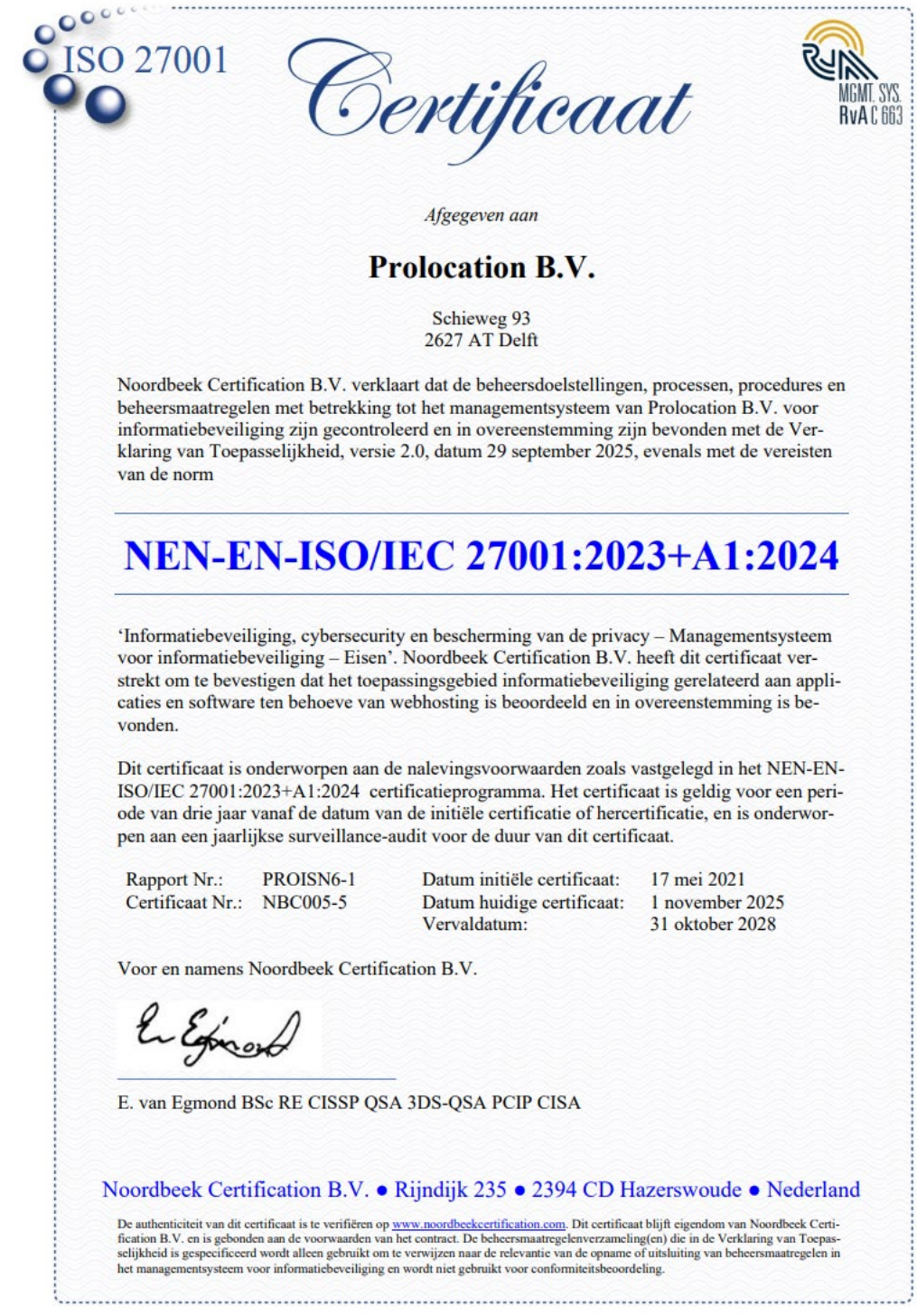
ID	Omschrijving	Naam beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag (Reden van insluiting)	NIS2/DORA relatie
		informatie moet worden gewist als deze niet langer nodig is.			☐ CV	
8.11	Maskeren van gegevens	Gegevens moeten worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels, en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving.	Ja		☑ RB ☐ WG ☐ CV	
8.12	Voorkomen van gegevenslekken (Data leakage prevention)	Maatregelen om gegevenslekken te voorkomen moeten worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.	Ja		☑ RB ☐ WG ☐ CV	
8.13	Back-up van informatie	Back-ups van informatie, software en systemen moeten worden bewaard en regelmatig worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (C) Business Continuity, such as backup management and disaster recovery and crisis management G) Basic cyber hygiene practices and cybersecurity training;
ZORG	Zorgspecifieke beheersmaatregel (aanvullend)		Ja		idem	
8.14	Redundantie van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (C) Business Continuity, such as backup management and disaster recovery and crisis management
8.15	Logging	Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (C) Business Continuity, such as backup management and disaster recovery and crisis management

ID	Omschrijving	Naam beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag (Reden van insluiting)	NIS2/DORA relatie
						G) Basic cyber hygiene practices and cybersecurity training;
8.16	Monitoren van activiteiten	Netwerken, systemen en toepassingen moeten worden gemonitord op afwijkend gedrag en er moeten passende maatregelen worden genomen om potentiële informatiebeveiligingsincidenten te evalueren.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (B) Incident handling (C) Business Continuity, such as backup management and disaster recovery and crisis management
8.17	Kloksynchronisatie	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdsbronnen.	Ja		☑ RB ☐ WG ☐ CV	
8.18	Gebruik van speciale systeemhulpmiddelen	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, moet worden beperkt en nauwkeurig te worden gecontroleerd.	Ja		☑ RB ☐ WG ☐ CV	
8.19	Installeren van software op operationele systemen	Er moeten procedures en maatregelen worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: (E) Security in network and information systems acquisitions, development and maintenance including vulnerability handling and disclosure G) Basic cyber hygiene practices and cybersecurity training;
8.20	Beveiliging netwerkcomponenten	Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja		☑ RB ☐ WG ☐ CV	
8.21	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en	Ja		☑ RB ☐ WG	

ID	Omschrijving	Naam beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag (Reden van insluiting)	NIS2/DORA relatie
		dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord.			☐ CV	
8.22	Netwerksegmentatie	Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: G) Basic cyber hygiene practices and cybersecurity training;
8.23	Toepassen van webfilters	De toegang tot externe websites moet worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.	Ja		☑ RB ☐ WG ☐ CV	
8.24	Gebruik van cryptografie	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, moeten worden gedefinieerd en geïmplementeerd.	Ja		☑ RB ☐ WG ☐ CV	Article 21: Cyber security risk management measures: H) Policies and procedures regarding the use of cryptography and, where appropriate, encryption;
8.25	Beveiligen tijdens de ontwikkelcyclus	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast.	Ja		☑ RB ☐ WG ☐ CV	
8.26	Toepassingsbeveiligingseisen	Er moeten eisen aan de informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	Ja		☑ RB ☐ WG ☐ CV	
8.27	Veilige systeemarchitectuur en technische uitgangspunten	Uitgangspunten voor het ontwerpen van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen.	Ja		☑ RB ☐ WG ☐ CV	
8.28	Veilig coderen	Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling.	Ja		☑ RB ☐ WG ☐ CV	

ID	Omschrijving	Naam beheersmaatregel	Relevant en geïmplementeerd	Onderbouwing uitsluiting	Grondslag (Reden van insluiting)	NIS2/DORA relatie
8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Processen voor het testen van de beveiliging moeten worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.	Ja		☑ RB ☐ WG ☐ CV	
8.30	Uitbestede systeemontwikkeling	De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.	Nee	Prolocation gebruikt geen derden voor het ontwikkelen van software.	☐ RB ☐ WG ☐ CV	
8.31	Scheiding van ontwikkel-, testen productieomgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd.	Ja		☑ RB ☐ WG ☐ CV	
8.32	Wijzigingsbeheer	Wijzigingen in informatieverwerkingsfaciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer.	Ja		☑ RB ☐ WG ☐ CV	
8.33	Testgegevens	Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.	Ja		☑ RB ☐ WG ☐ CV	
8.34	Bescherming van informatiesystemen tijdens audits	Audits en andere borgingsactiviteiten waarbij operationele systemen worden beoordeeld moeten worden gepland en overeengekomen tussen de tester en het verantwoordelijke management.	Ja		☑ RB ☐ WG ☐ CV	
8.35	HLT – Zero trust-beginselen	Zorgspecifieke beheersmaatregel	Ja		☑ RB ☐ WG ☐ CV	

Certificaten



ISO 27001

Certificaat

MGMT. SYS. RvA C 663

Afgegeven aan

Prolocation B.V.

Schieweg 93
2627 AT Delft

Noordbeek Certification B.V. verklaart dat de beheersdoelstellingen, processen, procedures en beheersmaatregelen met betrekking tot het managementsysteem van Prolocation B.V. voor informatiebeveiliging zijn gecontroleerd en in overeenstemming zijn bevonden met de Verklaring van Toepasselijkheid, versie 2.0, datum 29 september 2025, evenals met de vereisten van de norm

NEN-EN-ISO/IEC 27001:2023+A1:2024

'Informatiebeveiliging, cybersecurity en bescherming van de privacy – Managementsysteem voor informatiebeveiliging – Eisen'. Noordbeek Certification B.V. heeft dit certificaat verstrekt om te bevestigen dat het toepassingsgebied informatiebeveiliging gerelateerd aan applicaties en software ten behoeve van webhosting is beoordeeld en in overeenstemming is bevonden.

Dit certificaat is onderworpen aan de nalevingsvoorwaarden zoals vastgelegd in het NEN-EN-ISO/IEC 27001:2023+A1:2024 certificatieprogramma. Het certificaat is geldig voor een periode van drie jaar vanaf de datum van de initiële certificatie of hercertificatie, en is onderworpen aan een jaarlijkse surveillance-audit voor de duur van dit certificaat.

Rapport Nr.:	PROISN6-1	Datum initiële certificaat:	17 mei 2021
Certificaat Nr.:	NBC005-5	Datum huidige certificaat:	1 november 2025
		Vervaldatum:	31 oktober 2028

Voor en namens Noordbeek Certification B.V.

E. van Egmond BSc RE CISSP QSA 3DS-QSA PCIP CISA

Noordbeek Certification B.V. ● Rijndijk 235 ● 2394 CD Hazerswoude ● Nederland

De authenticiteit van dit certificaat is te verifiëren op www.noordbeekcertification.com. Dit certificaat blijft eigendom van Noordbeek Certification B.V. en is gebonden aan de voorwaarden van het contract. De beheersmaatregelenverzameling(en) die in de Verklaring van Toepasselijkheid is gespecificeerd wordt alleen gebruikt om te verwijzen naar de relevantie van de opname of uitsluiting van beheersmaatregelen in het managementsysteem voor informatiebeveiliging en wordt niet gebruikt voor conformiteitsbeoordeling.

NEN 7510

Certificaat

NEN 7510
Informatiebeveiliging in de zorg

MGMT. SYS.
RvA C 663

Afgegeven aan

Prolocation B.V.

Schieweg 93
2627 AT Delft

Noordbeek Certification B.V. verklaart dat het door Prolocation B.V. gehanteerde managementsysteem voor informatiebeveiliging in de gezondheidszorg en de toepassing daarvan voldoen aan de eisen gesteld in

NEN 7510-1:2024

'Medische informatica - Informatiebeveiliging in de zorg - Deel 1: Managementsysteem', voor het toepassingsgebied informatiebeveiliging gerelateerd aan applicaties en software ten behoeve van webhosting, conform de Verklaring van Toepasselijkheid, versie 2.0, gedateerd 29 september 2025.

Aan dit certificaat zijn nalevingsvoorwaarden verbonden zoals vastgelegd in het certificeringsprogramma NEN 7510-1:2024. Het certificaat is geldig voor een periode van drie jaar vanaf de datum van de initiële certificatie of hercertificatie, en is onderworpen aan een jaarlijkse surveillance-audit voor de duur van dit certificaat.

Rapport Nr.:	PROISN6-1	Datum initiële certificaat:	17 mei 2021
Certificaat Nr.:	NBC006-5	Datum huidige certificaat:	1 november 2025
		Vervaldatum:	31 oktober 2028

Voor en namens Noordbeek Certification B.V.

E. van Egmond BSc RE CISSP QSA 3DS-QSA PCIP CISA

Noordbeek Certification B.V. ● Rijndijk 235 ● 2394 CD Hazerswoude ● Nederland

Checklist wederzijdse afspraken

Onderwerp	Taak	Status
Afhankelijkheden	Bespreken waar de afhankelijkheden en risico's in de keten zitten, mogelijke gevolgen en eventuele uitwijkmogelijkheden. Mogelijke scenario's: 1. Levering is niet meer mogelijk als gevolg van een digitale aanval; 2. Een van de partijen in de keten is gehackt en hierdoor heeft de aanvaller mogelijk ook toegang tot (digitale) systemen; 3. Er is een kritieke kwetsbaarheid ontdekt in één van de (digitale) producten of diensten die worden gebruikt in het bedrijfsproces.	
(Gedeelde) Rollen en verantwoordelijkheden	Voldoende helder vastgelegd (bijv. wie mag wijzigingen aanmelden etc.) . Wie wordt geïnformeerd bij incidenten , datalekken of ernstige dreigingen, onderhoud.	
Afspraken (wederzijds)	Incidentmeldingen en support bij incidenten	
	Back-ups, frequentie, retentie, afwijkingen, restore	
	Toegangscontrole, wederzijds informeren bij wijzigingen in key-functies	
	Teruggave of verwijdering van activa, heldere afspraken bij offboarden klant/site	
	Onderhoudsafspraken, wie informeert wie, wanneer en hoe?	
	Pentestafspraken en betreffende omgeving	
Overige afspraken		