

Global Network Group

GDPR verwerkersverklaring

Alle verwijzingen in deze verwerkersverklaring zijn op basis van de geldige versie.

Alle openbare documenten zijn gepubliceerd op onze websites.

Vragen?

Neem contact met ons op via het contactformulier op de website of bel via:

Duitsland: +49(0)2822 961 6053

Nederland: +31(0)88 0038 780

Verenigd Koninkrijk: +44(0)1904 911 305

Zuid Afrika: +27(0)10 900 4749

Document code: GNG.RD.007.NL

Goedgekeurd door: ICC Council

Versie: V2 – Januari 2022

Status: Goedgekeurd



ALGEMENE BEPALINGEN

Op de verwerkingsverklaring GNG.RD.007.NL zijn de volgende documenten van toepassing:

1. Document GNG.RD.001.INT List of terms and definitions
2. Document GNG.RD.002.NL Algemene voorwaarden
3. Document GNG.RD.003.NL Algemene bepalingen voor alle documenten
4. Document GNG.RD.005.NL Privacy verklaring Global Network Group

De hiervoor genoemde documenten staan gepubliceerd op onze websites en zijn hierbij als herhaald en ingelast aangemerkt.

INHOUDSOPGAVE

ALGEMENE BEPALINGEN.....	2
INHOUDSOPGAVE.....	2
A.Partijen	4
B.Overwegingen	4
1.Karakter en duur van de verwerkersverklaring.....	5
2.Scope van de verwerkersverklaring	5
3.Het verwerken en gebruik van de persoonsgegevens.....	5
4.Geheimhouding	6
5.Beveiliging	6
6.Audit.....	7
7.Datalek (Personal Data Breach – Verordening (EU) 2017/679 artikel 4 lid 12)	7
8.Procedure meldplicht datalekken.....	8
9.Verzoeken van betrokkenen	8
10.Sub-verwerkers	9
11.Toegang tot de persoonsgegevens	9
12.Aansprakelijkheid en vrijwaring	9
13.Beëindiging en gevolgen van beëindiging	10
14.Gevolgen van nietigheid of vernietigbaarheid.....	10
15.Privacy verklaring Global Network Group.....	10
16.Toepasselijk(e) taal, recht en bevoegde rechter	10
Annex A Verwerkingsregister	11
A1.Gegevens van de verwerker	11
A2.Algemene verwerkingsactiviteiten	11
A3.Verwerkingsactiviteiten van bijzondere persoonsgegevens	11
Annex B Protocol meldplicht datalekken.....	12
B1.Algemeen	12
B2.Definitie datalek	12
B3.Interne verantwoordelijke melding datalekken	12
B4.Interne melding bij ontdekking van een datalek.....	12

B5.Onderzoek door de interne verantwoordelijke	13
B6.Bestrijding datalek	13
B7.Vaststelling van de gevolgen van een datalek	13
B8.Medewerking verstrekking gegevens omtrent het datalek	13
B9.Beschikbaarheid personeel na ontdekking datalek	14
B10.Beslissing melding datalekken	14
B11.Melding datalekken aan de Autoriteit Persoonsgegevens en/of betrokkenen	14
B12.Gevolgen melding datalekken	15
B13.Bijhouden register datalekken	15
Annex C Document GNG.RD.005 Privacy verklaring Global Network Group	16

A.Partijen

1. De door Global Network Group geaccrediteerde opleidingsinstituten, hierna te noemen '**verantwoordelijken**'
2. De door Global Network Group aangestelde ambassadeurs, hierna te noemen '**verantwoordelijken**'
3. Global Network Group, mede handelend als ADR Platform, ADR Register, EMCI Register en ICR Coach Register, hierna te noemen '**verwerker**'

B.Overwegingen

1. De Verordening (EU) 2017/679 (GDPR – General Data Protection Regulation) verplicht de verwerker om de (persoons)gegevens van de verantwoordelijken op basis van een overeenkomst of anderszins verkregen toestemming te verwerken.
2. Global Network Group handelt tegen Nederlands recht zodat de verordening (EU) 2017/679 van toepassing is.
3. De verwerking van de (persoons)gegevens komt voort uit de samenwerking van de certificeringsinstantie Global Network Group instantie met de door Global Network Group geaccrediteerde opleidingsinstituten en de door Global Network Group benoemde ambassadeurs, voor zover e.e.a. blijkt uit een overeenkomst of anderszins tot stand gekomen afspraken tussen partijen.
4. De partijen zijn gehouden afspraken te maken met betrekking tot het waarborgen van de privacy van persoonsgegevens en vast te leggen in een verwerkersovereenkomst, of anderszins te bevestigen, en kiezen ervoor e.e.a. via deze verwerkersverklaring te regelen.
5. De partijen zullen elkaar over en weer tijdig alle benodigde informatie verstrekken om een goede naleving van de GDPR en de nationaal geldende privacywet- en regelgeving mogelijk te maken.
6. De bepalingen van deze verwerkersverklaring gaan vóór alle andere afspraken die tussen partijen gelden ten aanzien van de verwerking van persoonsgegevens, indien en voor zover zij afwijken van hetgeen in deze verwerkersverklaring is vastgelegd.

1.Karakter en duur van de verwerkersverklaring

- 1.1. De verwerkersverklaring komt voort uit de Verordening (EU) 2016/679, speciek artikel 28 lid 3.
- 1.2. De verwerkingsverklaring is vastgesteld tegen de Global Network Group documentcode GNG.RD.007 entreedt in werking tegen het versie nummer zoals benoemd op pagina 1, en de aan dit versie nummer gekoppelde ingangsdatum. Uitsluitend de verwerkersverklaring met een geldig versie nummer is van toepassing.
- 1.3. De verwerkersverklaring is de bevestiging van de verwerker aan de verantwoordelijken en heeft het karakter van een overeenkomst (juncto artikel 1 lid 4).
- 1.4. De verwerkingsverklaring is onlosmakelijk onderdeel van:
 - 1) de samenwerkingsovereenkomst tussen Global Network Group en het opleidingsinstituut of de ambassadeur, *of*
 - 2) het accreditatie besluit van het opleidingsinstituut, *of*
 - 3) het benoemingsbesluit van de ambassadeur, *of*
 - 4) ieder ander document dat de samenwerking tussen de partijen regelt, zulks ter beoordeling van Global Network Group.
- 1.5. De verwerkersverklaring eindigt nadat verwerker alle persoonsgegevens waar het betrekking op heeft, heeft gewist en/of terugbezorgd overeenkomstig het bepaalde in artikel 13.
- 1.6. De verwerkersverklaring kan niet tussentijds worden opgezegd.
- 1.7. De bepalingen zoals omschreven in artikel 4 zijn altijd geldig, zelfs indien de verwerkersverklaring buiten werking is gesteld.

2.Scope van de verwerkersverklaring

- 2.1. De scope van de verwerkersverklaring is vastgelegd in het verwerkingsregister (Annex A).

3.Het verwerken en gebruik van de persoonsgegevens

- 3.1. Het doel van de verwerking en welke persoonsgegevens worden verwerkt is door partijen bepaald en blijkt uit de verwerkingsverklaring.
- 3.2. De verantwoordelijken kunnen hiertoe schriftelijke instructies uitgeven aan de verwerker.
- 3.3. De verwerker gebruikt de verkregen persoonsgegevens alleen voor de doeleinden waarvoor ze zijn verstrekt en indien uitgegeven uitsluitend volgens de schriftelijke instructies van de verantwoordelijken.
- 3.4. Indien de verantwoordelijken opdracht geven om de persoonsgegevens te verwerken op een wijze die volgens de verwerker in strijd is met de wettelijke verplichtingen, dan informeert laatstgenoemde (verwerker) de verantwoordelijken hieromtrent en overlegt de verwerker met de verantwoordelijken om tot een oplossing te komen die niet in strijd is met de wettelijke verplichtingen.

-
- 3.5. De verwerker heeft een eigen verantwoordelijkheid om de gegevens niet in strijd met de geldende wet- en regelgeving te verwerken.
 - 3.6. De verwerker zal de persoonsgegevens niet aan derden verstrekken, tenzij dit gebeurt in opdracht van de verantwoordelijken of wanneer dit noodzakelijk is om te voldoen aan een wettelijke verplichting.
 - 3.7. De verwerker verwerkt de persoonsgegevens binnen de Europese Economische Ruimte en in de navolgende landen: Duitsland, Nederland, Verenigd Koninkrijk, Verenigde Staten van Amerika, Zuid Afrika.

4. Geheimhouding

- 4.1. De verwerker treft alle noodzakelijke maatregelen om geheimhouding van de persoonsgegevens van de verantwoordelijken te waarborgen.
- 4.2. De in lid 1 gestelde verplichting geldt niet wanneer de verantwoordelijken voorafgaande schriftelijke toestemming hebben gegeven om de persoonsgegevens aan een derde te verstrekken of wanneer de verwerker hiertoe wettelijk verplicht is.
- 4.3. Een derde of subverwerker is niet een door de verwerker ingeschakelde leverancier (externe provider) van de (noodzakelijke) (technische) systemen t.b.v. de administratieve en operationele verwerking van de persoonsgegevens.
- 4.4. De verwerker zal dezelfde geheimhoudingsplicht opleggen aan diens personeel c.q. hiervoor ingeschakelde personen of sub-verwerkers.
- 4.5. Bij overtreding van dit artikel, verbeurt de verwerker een onmiddellijk opeisbare boete van € 100,- per overtreding aan de verantwoordelijken, onverminderd het recht van verantwoordelijken om volledige schadevergoeding te vorderen.

5. Beveiliging

- 5.1. De verantwoordelijken en de verwerker zullen beiden passende technische en organisatorische maatregelen treffen, zodat zij een op het risico afgestemd beveiligingsniveau kunnen waarborgen.
- 5.2. De verantwoordelijken informeren de verwerker omtrent de wettelijke betrouwbaarheidseisen die op de verwerking van toepassing zijn aan de hand van de mogelijke gevolgen voor de betrokkenen, zoals in geval van verlies, corruptie of onrechtmatige verwerking en verstrekt daartoe alle benodigde informatie zodat de verwerker hieraan kan voldoen.
- 5.3. Indien de verantwoordelijken een hoger beveiligingsniveau wensen dan gangbaar/gebruikelijk, kan de verwerker hiervoor de redelijke kosten separaat in rekening brengen aan de verantwoordelijken.

-
- 5.4. 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.
 - 5.5. Indien de verantwoordelijken een beoordeling wensen uit te voeren van een beoogde verwerkingsactiviteit, verleent de verwerker alle redelijke medewerking om deze beoordeling in overeenstemming met de GDPR uit te voeren.
 - 5.6. De verwerker verleent eveneens alle redelijke medewerking aan een voorafgaande raadpleging van de Autoriteit Persoonsgegevens.
 - 5.7. De voor de uitvoering van de verwerkersverklaring noodzakelijke technische en organisatorische beveiligingsmaatregelen zijn benoemd in het verwerkingsregister (Annex A).

6.Audit

- 6.1. De verantwoordelijken hebben het recht om jaarlijks op eigen kosten een audit te laten uitvoeren ter controle op de naleving van de verwerkersverklaring. De audit is beperkt tot de scope GDPR en heeft een vertrouwelijk, niet openbaar karakter. De auditoren dienen GDPR deskundig te zijn, zulks ter beoordeling van Global Network Group, en zijn verplicht een geheimhoudingsverklaring te ondertekenen.
- 6.2. 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.
- 6.3. De verwerker voert de aanbevelingen die uit de audit zijn gekomen in overleg met de verantwoordelijken zo spoedig mogelijk uit.
- 6.4. Indien de aanpassingen als gevolg van lid 3 voortkomen uit gewijzigde inzichten of wetgeving, dan zijn de redelijke kosten voor deze aanpassingen voor de verantwoordelijken.
- 6.5. Indien de aanpassingen als gevolg van lid 3 voortkomen uit een tekortkoming in de nakoming van de GDPR, dan zijn deze kosten voor de verwerker.
- 6.6. 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 verantwoordelijken hieromtrent zo snel mogelijk van op de hoogte.

7.Datalek (Personal Data Breach – Verordening (EU) 2017/679 artikel 4 lid 12)

- 7.1. Indien zich een GDPR gerelateerd datalek voordoet informeert de verwerker de verantwoordelijken hieromtrent op de wijze zoals verder omschreven in artikel 8. Zie ook Annex B onder B2.

-
- 7.2. In geval van een datalek treft de verwerker alle redelijke noodzakelijke maatregelen om de gevolgen hiervan te beperken en een nieuw lek te voorkomen.
 - 7.3. De verwerker verleent de verantwoordelijken 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.
 - 7.4. Partijen hebben hun afspraken over de te volgen procedure in geval van een datalek vastgelegd in een procedure meldplicht datalekken, zoals omschreven in artikel 8. Deze procedure kan worden aangepast indien de stand van de techniek dit verlangt of de regelgeving omtrent de meldplicht datalekken wijzigt.
 - 7.5. Indien de verwerker nalaat het datalek tijdig te melden conform de procedure meldplicht datalekken zoals bedoeld in artikel 8, is hij een direct opeisbare boete van € 100,- verschuldigd aan de verantwoordelijken vermeerderd met 2% van dit bedrag per uur dat de melding te laat geschiedt.

8.Procedure meldplicht datalekken

- 8.1. De procedure is vastgelegd in het protocol meldplicht datalekken (Annex B).

9.Verzoeken van betrokkenen

- 9.1. Ieder verzoek tot inzage, rectificatie, gegevenswissing, beperking van de verwerking, overdraagbaarheid van gegevens of bezwaar dat de verwerker bereikt, stuurt hij onverwijld door aan de verantwoordelijken.
- 9.2. De verwerker verleent de verantwoordelijken alle redelijke medewerking zodat laatstgenoemden binnen de wettelijke termijnen kan voldoen aan een verzoek zoals bedoeld in lid 1.
- 9.3. De verantwoordelijken zullen de redelijke kosten die een dergelijke medewerking met zich meebrengt aan de verwerker vergoeden.
- 9.4. Met betrekking tot een verzoek zoals bedoeld in lid 1 geldt dat de verwerker de inwilliging en uitvoering ervan mogelijk niet, of niet volledig, in eigen hand heeft voor wat betreft elementen waarvoor de verwerker geheel of gedeeltelijk afhankelijk is van de ingeschakelde leverancier (externe provider) van de (noodzakelijke) (technische) systemen t.b.v. de administratieve en operationele verwerking van de persoonsgegevens.

10.Sub-verwerkers

- 10.1. De verwerker is niet gerechtigd om sub-verwerkers in te schakelen voor het verwerken van de persoonsgegevens uit de verwerkersverklaring, tenzij de verwerker hiervoor voorafgaande schriftelijke toestemming heeft gekregen (juncto artikel 4 lid 3 m.b.t. de uitsluiting van leveranciers van technische systemen).
- 10.2. De verwerker is verantwoordelijk en aansprakelijk voor de handelingen van door hem ingeschakelde sub-verwerkers.
- 10.3. Indien een verwerker een sub-verwerker inschakelt is hij verplicht te bedingen dat deze sub-verwerker alle bij de verwerkersverklaring opgelegde verplichtingen aan de verwerker nakomt en zal daartoe met de betreffende sub-verwerkers een overeenkomst sluiten die in overeenstemming is met de verwerkersverklaring.
- 10.4. Indien de verwerker zonder de toestemming zoals bedoeld in lid 1 sub-verwerkers inschakelt, is de verwerker een boete verschuldigd van € 100,- onverminderd het recht van de verantwoordelijken op volledige schadevergoeding, voor zover schade is ontstaan en kan worden aangetoond.

11.Toegang tot de persoonsgegevens

- 11.1. De verwerker zorgt in redelijkheid ervoor dat de verantwoordelijken te allen tijde toegang houden tot de betreffende persoonsgegevens, en verleent hiertoe alle medewerking in geval van zijn faillissement of surséance van betaling. Het voorgaande onder voorbehoud van force majeure.

12.Aansprakelijkheid en vrijwaring

- 12.1. De verwerker is niet verantwoordelijk voor schade als gevolg van schendingen van enige wet- of regelgeving door de verantwoordelijken.
- 12.2. De verantwoordelijken vrijwaren de verwerker voor aanspraken van derden en door verwerker gemaakte kosten als gevolg van een schending zoals bedoeld in lid 1.
- 12.3. De verantwoordelijken zijn niet verantwoordelijk voor schade als gevolg van schendingen van enige wet- of regelgeving door de verwerker.
- 12.4. De verwerker vrijwaart de verantwoordelijken voor aanspraken van derden en door verantwoordelijken gemaakte kosten als gevolg van een schending zoals bedoeld in lid 3.
- 12.5. De andere partij, is in een geval als bedoeld in lid 1 of 3, gerechtigd de samenwerking met onmiddellijke ingang op te zeggen.

13. Beëindiging en gevolgen van beëindiging

- 13.1. De werking van de verwerkersverklaring eindigt pas nadat de onderliggende accreditatie of benoeming is beëindigd én de verwerker alle aan hem verstrekte persoonsgegevens heeft overgedragen aan de verantwoordelijken of aan een door verantwoordelijken voorafgaand schriftelijk aangewezen derde, alsook alle achtergebleven gegevens bij de verwerker en diens eventuele sub-verwerkers zijn vernietigd.
- 13.2. Op verzoek van de verantwoordelijken 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.
- 13.3. In plaats van overdraging van de gegevens kunnen de verantwoordelijken de verwerker ook verzoeken om de gegevens te vernietigen. Onder vernietigen wordt verstaan het verwijderen uit alle administratieve en technische systemen.
- 13.4. Vernietiging van de gegevens zoals bedoeld in lid 3 kan pas plaatsvinden nadat de verantwoordelijken hiervoor voorafgaande schriftelijke toestemming hebben gegeven.
- 13.5. De bepalingen van artikel 4 blijven echter onverminderd van kracht.

14. Gevolgen van nietigheid of vernietigbaarheid

- 14.1. Indien een deel van de verwerkersverklaring nietig of vernietigbaar is, dan tast dit de overige bepalingen in de verwerkersverklaring 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 bij het opstellen van de verwerkersverklaring werd beoogd.

15. Privacy verklaring Global Network Group

- 15.1. Het document GNG.RD.005 Privacy verklaring is van toepassing op de verwerkersverklaring en wordt hierbij als herhaald en ingelast aangemerkt (Annex C).

16. Toepasselijk(e) taal, recht en bevoegde rechter

- 16.1. Op de verwerkersverklaring is uitsluitend Nederlands recht van toepassing.
- 16.2. Bij meertaligheid prefereert de Nederlandse taal.
- 16.3. Alle eventuele geschillen die ontstaan naar aanleiding van de verwerkersverklaring en die niet via mediation kunnen worden opgelost worden voorgelegd aan een arbiter of de bevoegde rechter.

Annex A Verwerkingsregister

A1. Gegevens van de verwerker

Bedrijfsnaam:	Global Network Group
Verantwoordelijk persoon:	de heer Giel Tettelaar
Website:	https://global-network-group.eu
Website ADR Platform:	https://adrplatform.com
Website ADR Register:	https://adr-register.com
Website EMCI Register:	https://emci-register.com
Website ICR Coach Register:	https://icr-coachregister.com
Telefoon:	+31(0)88 0038 780
Toepasselijk(e) recht & taal:	Nederlands recht, Nederlandse taal

A2. Algemene verwerkingsactiviteiten

Categorie persoonsgegevens(s):	<u>via opgave door het opleidingsinstituut of de ambassadeur</u> namen + emailadressen, incidenteel ook titelatuur, adressen, woonplaatsen, telefoonnummers, gegevens van de bij het trainingsinstituut gevolgde opleidingen
Categorie betrokkenen:	<u>personen</u> (oud) studenten/deelnemers van geaccrediteerde opleidingsinstututen (studenten/deelnemers van niet geaccrediteerde opleidingsinstututen zijn uitgesloten) + relaties/contacten van ambassadeurs
Grondslag voor de verwerking:	<u>toestemming</u> op basis van de accreditatie van het opleidingsinstituut of de benoeming als ambassadeur
Doel verwerking:	<u>dienstverlening</u> het informeren en voorlichten van de (oud) studenten/deelnemers, relaties en contacten m.b.t. de dienstverlening van Global Network Group als certificeringsinstantie.
Zelf verwerken:	ja
Waar bevindt zich de verwerker?	binnen de Europese Economische Ruimte en in de navolgende landen: Duitsland, Nederland, Verenigd Koninkrijk, Verenigde Staten van Amerika, Zuid Afrika.
EU Verwerkersovereenkomst?	ja, verwerkersverklaring GNG.RD.007
Bewaartermijn:	onbepaalde tijd
Veiligheidsmaatregelen:	ja – uitsluitend GDPR gekwalificeerde systemen worden toegepast, zulks blijktens de (conformiteits) opgave van de leverancier of ter beoordeling van Global Network Group

A3. Verwerkingsactiviteiten van bijzondere persoonsgegevens

Niet van toepassing

Annex B Protocol meldplicht datalekken

B1. Algemeen

- Global Network Group hecht belang aan een goede beveiliging van haar (elektronische) systemen waarin persoonsgegevens zijn opgeslagen en worden verwerkt.
- Het valt desalniettemin nooit volledig te voorkomen dat een datalek zal plaatsvinden.
- Global Network Group is verplicht om (ernstige) datalekken te melden aan de Autoriteit Persoonsgegevens en aan de betrokkenen.
- Global Network Group wenst aan haar wettelijke verplichtingen te voldoen.
- Global Network Group heeft daarom het beleid zoals opgenomen in deze Annex B geformuleerd om zo adequaat mogelijk te handelen indien onverhoopt een datalek plaatsvindt.

B2. Definitie datalek

- Er is sprake van een datalek als er een inbreuk op de beveiliging plaatsvindt die per ongeluk of op onrechtmatige wijze leidt tot vernietiging, verlies, wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens (zie Verordening (EU) 2017/679 artikel 4 lid 12, alsmede artikel 7 van de verwerkersverklaring).

B3. Interne verantwoordelijke melding datalekken

- Global Network Group heeft een interne verantwoordelijke voor de verwerking van datalekken aangesteld die verantwoordelijk is voor de melding van een datalek.
- Deze verantwoordelijke is de heer Giel Tettelaar, hierna te noemen: 'interne verantwoordelijke'.

B4. Interne melding bij ontdekking van een datalek

- Degene die een datalek bij GNG ontdekt, meldt dit per omgaande aan de interne verantwoordelijke.
- Indien mogelijk en altijd in samenspraak met en na verkregen toestemming van de interne verantwoordelijke, zorgt degene die het datalek heeft ontdekt er gelijktijdig voor dat de gelekte gegevens zo snel als mogelijk op afstand worden gewist of ontoegankelijk gemaakt.

B5.Onderzoek door de interne verantwoordelijke

- De interne verantwoordelijke onderzoekt onder meer:
 - scope, oorzaak, omvang en impact van het datalek alsmede (noodzakelijke) preventieve en correctieve actie
 - welke persoonsgegevens verloren zijn gegaan of deze onrechtmatig gebruikt (kunnen) worden
 - wie of welke afdelingen binnen de organisatie betrokken zijn bij het datalek
 - welke sub-verwerker(s) en derden betrokken zijn bij het incident

B6.Bestrijding datalek

- De interne verantwoordelijke stopt het datalek indien dat nog kan en neemt voorts de noodzakelijke maatregelen om het datalek zo goed mogelijk te bestrijden.

B7.Vaststelling van de gevolgen van een datalek

- De interne verantwoordelijke onderzoekt de mogelijke gevolgen van het datalek aan de hand van de aard en de omvang van de gegevens die gelekt zijn en stelt vast wat de nadelige gevolgen van de betrokkenen kan zijn.

B8.Medewerking verstrekking gegevens omtrent het datalek

- De ontdekker/melder van het datalek biedt alle medewerking aan de interne verantwoordelijk door zo snel en zo goed mogelijk (schriftelijk) antwoord te geven op de volgende vragen:
 - wat is er gebeurd? (omschrijving van het incident)
 - ging het per ongeluk of is het veroorzaakt door kwade opzet (denk aan gehackte gegevens)?
 - wanneer is het gebeurd? (datum en tijdstip)
 - wanneer is het ontdekt?
 - wat voor gegevens zijn gelekt?
 - zijn de gegevens versleuteld, en zo ja hoe?
 - wat is het effect?
 - wat is de omvang?
 - wat is de impact?
 - konden de gegevens op afstand worden gewist of ontoegankelijk gemaakt, en zo ja, is dat gebeurd?
 - wat zijn de mogelijke gevolgen voor de betrokkenen?
 - welke groep(en) personen is/zijn hierdoor getroffen, en wat is hun omvang?
 - konden er al technische en/of organisatorische maatregelen worden getroffen naar aanleiding van het incident?

B9. Beschikbaarheid personeel na ontdekking datalek

- De verantwoordelijke van de afdeling vanuit waar het datalek heeft plaatsgevonden alsook de ontdekker van het datalek en iedereen die vanuit hun functie of kennis in staat is om organisatorische en/of technische maatregelen te treffen om de gevolgen van het datalek te beperken, houden zich de 1e 24 uur na ontdekking van het datalek beschikbaar voor overleg met de interne verantwoordelijke c.q. eventueel door hem aangewezen experts en voor het zo nodig uitvoeren van opgedragen werkzaamheden als gevolg van het datalek.

B10. Beslissing melding datalekken

- De interne verantwoordelijke beslist zo spoedig mogelijk doch in elk geval binnen 60 uur na ontdekking van het datalek - al dan niet in overleg met de verantwoordelijke van de afdeling vanuit waar het datalek is ontdekt en/of door hem aangewezen experts - of het datalek dient te worden gemeld aan de Autoriteit Persoonsgegevens en/of de betrokkenen.
- Een datalek wordt in principe altijd gemeld aan de Autoriteit Persoonsgegevens, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van de betrokkenen.
- De melding van het datalek gaat gepaard met beantwoording van de vragen zoals omschreven in onderdeel B8.
- Een datalek dat gemeld is aan de Autoriteit Persoonsgegeven wordt eveneens gemeld aan de betrokkenen indien het een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, tenzij inmiddels passende maatregelen zijn genomen dat het hoge risico heeft afgewend.

B11. Melding datalekken aan de Autoriteit Persoonsgegevens en/of betrokkenen

- De interne verantwoordelijke draagt zo nodig zorg voor de melding aan de Autoriteit Persoonsgegevens en/of de betrokkene(n).
- Melding geschiedt zo spoedig mogelijk na de ontdekking en uiterlijk binnen 72 uur na ontdekking van het datalek.
- Het is enige andere werknemer dan de interne verantwoordelijke niet toegestaan om het (mogelijke) datalek zelf aan de Autoriteit Persoonsgegevens en/of de betrokkene(n) te melden.
- Als een werknemer het niet eens is met de beslissing van de interne verantwoordelijke omtrent het al dan niet melden van het datalek aan de Autoriteit Persoonsgegevens en/of de betrokkene(n), dan kan hij/zij de grieven kenbaar maken aan de directie.
- Indien daartoe verzocht, verleent een werknemer alle medewerking aan de verantwoordelijke om de getroffen personen te kunnen informeren omtrent het datalek.

B12. Gevolgen melding datalekken

- Indien het datalek negatieve gevolgen heeft voor betrokkenen, dan doet de interne verantwoordelijke er alles aan om deze gevolgen zoveel mogelijk te beperken.
- Afhankelijk van de aard en de omvang van het datalek voor betrokkenen bepaalt de interne verantwoordelijke:
 - op welke wijze betrokkenen worden geïnformeerd (waaronder in ieder geval de mededelingen worden gedaan welke soorten persoonsgegevens getroffen zijn, wat de mogelijke gevolgen zijn, welke maatregelen GNG neemt en op welke wijze betrokkenen zelf de schade kunnen voorkomen of beperken)
 - welke nazorg betrokkenen krijgen
 - welke acties in het belang van de organisatie noodzakelijk zijn
- Indien een datalek heeft plaatsgevonden - ongeacht of deze is gemeld of niet - worden zo spoedig mogelijk adequate technische en/of organisatorische maatregelen getroffen om toekomstige gelijksoortige datalekken te voorkomen.

B13. Bijhouden register datalekken

- De interne verantwoordelijke houdt een overzicht bij van alle datalekken, waarin alle gegevens rondom het datalek worden geregistreerd, zoals:
 - een omschrijving van het incident
 - datum en tijdstip van het datalek
 - datum en tijdstip ontdekking van het datalek
 - omschrijving van scope, oorzaak, omvang, impact
 - omschrijving van de categorie(en) van betrokkenen die zijn getroffen
 - omschrijving aantal betrokkenen (bij benadering)
 - of het incident is gemeld aan de Autoriteit Persoonsgegevens en zo ja datum en tijdstip melding
 - of het incident is gemeld aan de betrokkenen en zo ja, datum en tijdstip melding
 - op welke wijze betrokkenen zijn geïnformeerd
 - de gevolgen van het datalek, met indien mogelijk vermelding van datum en tijdstip
 - welke technische en/of organisatorische maatregelen zijn getroffen na het datalek, met vermelding van datum en tijdstip
- Onder overzicht wordt verstaan:
 - opname in interne audits rapportages, of
 - opname in CPAR rapportages, of
 - opname in de jaarlijkse management review, of
 - andere wijze van bijhouden ter beoordeling van Global Network Group.

Annex C Document GNG.RD.005 Privacy verklaring Global Network Group

Global Network Group

Privacy verklaring

Alle verwijzingen in dit document zijn op basis van de geldige versie.

Alle openbare documenten zijn gepubliceerd op onze websites.

Vragen?

Neem contact met ons op via het contactformulier op de website of bel via:

Duitsland: +49(0)2822 961 6053

Nederland: +31(0)88 0038 780

Verenigd Koninkrijk: +44(0)1904 911 305

Zuid Afrika: +27(0)10 900 4749

Document code: GNG.RD.005.NL

Goedgekeurd door: ICC Council

Versie: V3 – Januari 2022

Status: Goedgekeurd



ALGEMENE BEPALINGEN

Op dit document GNG.RD.005.NL zijn de volgende documenten van toepassing:

1. Document GNG.RD.001.INT List of terms and definitions
2. Document GNG.RD.002.NL Algemene voorwaarden
3. Document GNG.RD.003.NL Algemene bepalingen voor alle documenten

De hiervoor genoemde documenten staan gepubliceerd op onze websites en zijn hierbij als herhaald en ingelast aangemerkt.

INHOUDSOPGAVE

ALGEMENE BEPALINGEN	2
INHOUDSOPGAVE	2
PRIVACY VERKLARING	3
1. Algemeen.....	3
2. Dochterondernemingen en handelsnamen.....	3
3. Toestemming.....	3
4. Gebruik van door ons verkregen informatie	4
4.1. Gebruikmaken van onze diensten.....	4
4.2. Communicatie	4
4.3. Type informatie en dossiers	4
4.4. Profieldossier.....	5
4.5. Certificeringsdossier	6
4.6. Cookies	7
4.7. Uitzetten cookies	7
4.8. Gebruik - doeleinden	7
4.9. Intern gebruik	7
4.10. Gebruik t.b.v. audits en onderzoek	7
4.11. Gebruik door geaccrediteerde opleidingsinstituten en ambassadeurs	7
4.12. Verkoop aan andere partijen	7
4.13. Gebruik door andere partijen.....	7
4.14. Aanpassingen	7
4.15. Keuzes ten aanzien van persoonlijke informatie	8
4.16. Aan- en afmelden voor nieuwsbrieven.....	8
5. Vragen en feedback	8

PRIVACY VERKLARING

1. Algemeen

Global Network Group is zich ervan bewust dat zij (Global Network Group) persoonlijke en vertrouwelijke informatie verzamelt. Global Network Group rekent het tot haar taak en zorg om hierin uw privacy te garanderen. Via deze Privacy Verklaring informeren wij u hoe we hieraan vorm en inhoud geven, hoe wij werken, welke informatie we waarom verzamelen en hoe we hiermee uw bezoekers- en klantervaring beogen te verbeteren.

Deze Privacy Verklaring is van toepassing op alle websites en dienstverlening van Global Network Group. Wij wijzen u erop dat Global Network Group niet verantwoordelijk is voor privacy beleid van andere websites en bronnen.

Op basis van het privacy beleid respecteert Global Network Group de privacy van al haar website gebruikers en cliënten (certificaathouders). Alle verkregen informatie wordt vertrouwelijk behandeld.

2. Dochterondernemingen en handelsnamen

Global Network Group houdt diverse werkmaatschappijen en handelsnamen, waaronder ADR Platform, ADR Register, ICR Coach Register en EMCI Register. Op allen is deze Privacy Verklaring van toepassing.

3. Toestemming

Iedere (kandidaat) certificaathouder (de aanmelder) is vanaf het moment van indiening (uploaden) van zijn/haar aanmelding automatisch akkoord met onze algemene voorwaarden en deze Privacy Verklaring.

Iedere bezoeker van onze website(s) gaat automatisch akkoord met onze algemene voorwaarden en deze Privacy Verklaring.

4. Gebruik van door ons verkregen informatie

4.1. Gebruikmaken van onze diensten

Wanneer u zich aanmeldt voor 1 van onze diensten vragen wij u om persoonlijke informatie. Deze informatie wordt uitsluitend gebruikt voor het uitvoeren van de afgenomen dienst(en). Alle informatie wordt opgeslagen op beveiligde servers van Global Network Group of van 1 van onze contractpartners. Global Network Group zal deze informatie niet koppelen aan of gebruiken in combinatie met andere informatie waarover wordt beschikt.

4.2. Communicatie

Communicatie en aan ons verstuurde correspondentie, in welke vorm dan ook, kan worden bewaard en opgeslagen. Soms wordt u gevraagd hierbij persoonlijke informatie aan te leveren die verband houdt met het onderwerp van de correspondentie. Op deze manier is mogelijk uw communicatie en correspondentie procesmatig en inhoudelijk correct af te behandelen. Alle informatie wordt opgeslagen op beveiligde servers van Global Network Group of van 1 van onze contractpartners. Global Network Group zal deze informatie niet koppelen aan of gebruiken in combinatie met andere informatie waarover wordt beschikt.

4.3. Type informatie en dossiers

Global Network Group verzamelt informatie met betrekking tot de accreditatie, certificering en registratie van personen, bedrijven, producten en diensten.

Hierbij worden twee informatie typen en dossiers onderscheiden, namelijk:

- informatie bedoeld voor publicatie in het (de) openbare profiel(en) van de (kandidaat) certificaathouder (profiel dossier) en
- informatie bedoeld voor de kwalificatie als certificaathouder alsmede het in stand houden van de registratie en certificering (certificerings dossier).

Global Network Group beheert de beide informatie typen / dossiers op gescheiden servers.

4.4. Profieldossier

Global Network Group houdt van iedere (kandidaat) certificaathouder een profiel dossier.

Dit dossier bevat:

- NAW gegevens van het bedrijf of de locatie waar de zakelijke activiteiten feitelijk worden uitgevoerd;
- Gegevens met betrekking tot telefoon, telefax, website;
- Contactformulier gekoppeld aan het persoonlijke of zakelijke emailadres van de certificaathouder;
- Links naar andere profielen & informatie, zoals social media, platforms, vergelijkingswebsites, marketing- en verkoopkanalen. Links kunnen worden geplaatst door Global Network Group of de certificaathouder.
- Logo's, foto's en informatie met betrekking tot de persoon en het bedrijf;
- Overige informatie verband houdend met de certificering;

Global Network Group vult profielen in op basis van het aanmeldingsformulier en social media links. Certificaathouders kunnen gegevens in het profieldossier, met uitzondering van certificaatgegevens, zelf beheren.

Het profieldossier is openbaar indien de certificaathouder beschikt over een geldige certificering.

Het profieldossier is openbaar indien de certificaathouder is geschorst of geroyeerd, echter voor een maximale tijdsduur van 5 aaneengesloten kalenjaren gerekend vanaf het ingaan van de schorsing of het royement.

Indien certificering wordt beëindigd door de certificaathouder of Global Network Group, of aan de certificaathouder wordt ontnomen, wordt het profieldossier voor onbepaalde tijd bewaard, tenzij de certificaathouder om verwijdering verzoekt.

4.5. Certificeringsdossier

Global Network Group houdt van iedere (kandidaat) certificaathouder een certificeringsdossier.

Dit dossier bevat:

- Alle correspondentie, documenten en informatie met betrekking tot het informeren over (via ondermeer campagnes en promotie uitingen, felicitatie berichten), de kwalificatie voor, en de instandhouding van de registratie en certificering;
- Alle correspondentie, documenten en informatie met betrekking tot de klanttevredenheid en de afhandeling van (disciplinaire) klachten en geschillen, indien verband houdend met de registratie en certificering;
- Overige correspondentie, documenten en informatie, indien verband houdend met de registratie en certificering.

Een certificeringsdossier is niet openbaar. Een certificeringsdossier is vertrouwelijk. Het uitvoeren van audits door bevoegde autoriteiten en toezichhouders is toegestaan.

Een certificeringsdossier wordt voor onbepaalde tijd aangehouden, ook na de beëindiging van de certificering, ongeacht de reden van de beëindiging.

Na de beëindiging van de certificering kan de certificaathouder verzoeken om het verwijderen van het certificeringsdossier. Global Network Group kan toestemming onthouden indien hiertoe aanleiding bestaat of indien de wet of een bevoegde autoriteit dit verlangt; in voorkomend geval is Global Network Group gehouden de certificaathouder dienaangaande te informeren. Onder alle omstandigheden dient de certificaathouder Global Network Group te vrijwaren van aansprakelijkheid indien het verwijderingsverzoek wordt toegewezen.

4.6.Cookies

Global Network Group verzamelt informatie met als doel de bezoekers en gebruikers van de website beter te begrijpen en van dienst te kunnen zijn. Deze website maakt gebruik van "cookies" zodat kan worden geanalyseerd hoe bezoekers de website gebruiken. De via "cookies" verkregen informatie kan worden doorgeleid of opgeslagen op beveiligde servers van Global Network Group of 1 van onze contractpartners. We gebruiken de verkregen informatie om uw website bezoek te evalueren, om (management) rapportages te maken en u gerelateerde diensten en producten aan te bieden.

4.7.Uitzetten cookies

De meest browsers accepteren automatisch cookies. We wijzen u erop dat u deze automatische acceptatie kunt uitzetten. Ook kunt u een melding aanzetten die u bericht wanneer cookies worden toegepast zodat u per cookie kunt besluiten over acceptatie of afwijzing. Het is mogelijk dat sommige functies van deze website niet of niet volledig functioneren of toegankelijk zijn indien cookies niet of beperkt worden geaccepteerd. Hiervoor maken we een voorbehoud.

4.8.Gebruik - doeleinden

Wij gebruiken de verkregen informatie niet voor andere doeleinden zoals beschreven in deze Privacy Verklaring tenzij we hiervoor separaat uw toestemming hebben verkregen.

4.9.Intern gebruik

De informatie wordt intern binnen Global Network Group en ICC Council gebruikt. Al onze medewerkers zijn verplicht de vertrouwelijk van uw gegevens en informatie te respecteren.

4.10.Gebruik t.b.v. audits en onderzoek

De informatie kan worden gebruikt ten behoeve van audits en onderzoeken uitgevoerd door bevoegde autoriteiten, toezichthouders, Global Network Group en ICC Council, dan wel andere organisaties hiertoe gemachtigd door 1 van de hiervoor genoemde organisaties. Wetenschappelijk onderzoek valt onder strekking van deze bepaling.

4.11.Samenwerking met geaccrediteerde opleidingsinstituten en ambassadeurs

Global Network Group werkt samen met geaccrediteerde opleidingsinstituten en ambassadeurs. Door Global Network Group geaccrediteerde opleidingsinstituten kunnen de informatie gebruiken. T.b.v. informatie en voorlichting m.b.t. de accreditatie, certificering en registratie verstrekken geaccrediteerde opleidingsinstituten de namen en emailadressen van de studenten van basis- en specialisatie opleidingen.

4.12.Verkoop aan andere partijen

Global Network Group verkoopt informatie niet door aan andere partijen, tenzij hiervoor specifiek toestemming voor is verkregen van de betreffende certificaathouders.

4.13.Gebruik door andere partijen

De informatie wordt niet gebruikt door andere partijen, tenzij hiervoor specifiek toestemming is verkregen van de betreffende certificaathouders.

4.14.Aanpassingen

Onze Privacy Verklaring is gericht op het gebruik en mogelijkheden van deze website en onze diensten. Iedere wijziging of aanpassing van deze website of onze diensten kan leiden tot aanpassing van onze Privacy Verklaring. Om deze reden adviseren wij u om tijdens ieder bezoek of gebruik van onze diensten kennis te nemen van onze disclaimer, algemene voorwaarden en privacy verklaring. Door het bezoeken van deze website of het gebruiken van onze diensten wordt u geacht hier uitvoering aan te hebben gegeven en akkoord te gaan met onze meest recente privacy verklaring. Hiervoor maken wij nadrukkelijk een voorbehoud.

4.15.Keuzes ten aanzien van persoonlijke informatie

Wij bieden onze cliënten (certificaathouders – geaccrediteerde of gecertificeerde bedrijven en organisaties) de mogelijkheid hun aan ons ter beschikking gestelde informatie te bekijken, te wijzigen of te verwijderen.

4.16.Aan- en afmelden voor nieuwsbrieven

Onder aan iedere nieuwsbrief bevindt zich een aan- en afmeldingsknop of instructie. Indien u uw gegevens zoals bij ons geregistreerd wilt wijzigen of verwijderen verzoeken wij u met ons contact op te nemen.

5.Vragen en feedback

Wij controleren regelmatig onze interne procedures met betrekking tot onze Privacy Verklaring. Indien u vragen of opmerkingen heeft verzoeken wij u met ons contact op te nemen.

U kunt contact opnemen via het contactformulier op onze website(s), door ons te bellen via +31(0)88 0038 780, of door een schriftelijke vraag te mailen of te zenden aan Global Network Group, ter attentie van de Quality Officer, Postbus 5530, 6802 EM Arnhem, Nederland.