PRIVACYVERKLARING

Telefoon +31(0)85 301 3010
Email info@hesqsupport.nl
Website www.hesqsupport.nl

Wij hechten zeer veel waarde aan het goed beschermen en het juist omgaan met uw persoonsgegevens. Per 25 mei 2018 is de Wet bescherming persoonsgegevens (Wbp) vervallen en wordt deze vervangen door de Algemene verordening gegevensbescherming (AVG). Deze wetgeving geldt voor de gehele Europese Unie.

Door middel van deze privacyverklaring maken wij inzichtelijk hoe wij uw persoonsgegevens beschermen en hoe wij hier op een juiste wijze mee omgaan.

In deze privacyverklaring zijn tevens de volgende zaken opgenomen:
- Beleid ten behoeve van informatiebeveiliging;
- Protocol voor afhandeling dataleken en beveiligingsincidenten;
- AVG-privacyrechten.

Persoonsgegevens die worden verwerkt

Binnen HESQ Support worden diverse persoonsgegevens verwerkt. Hieronder zal worden toegelicht welke gegevens worden verwerkt inclusief motivatie waarvoor wij deze gegevens gebruiken alsmede de bewaartermijn.

Onderdeel	Gegevens	Doel	Bewaartermijn
Facturatiegegevens*	-Bedrijfsnaam -Geadresseerde -Postadres -BTW nummer -Rekeningnummer -Uitvoering werkzaamheden (met vermelding van namen van kandidaten en uitvoeringsdatum)	-Voldoen aan belastingwet -Heldere facturatie waarbij traceerbaar is welke activiteiten zijn uitgevoerd en welke kandidaten hebben deelgenomen aan trainingen -Opnemen van contact in relatie tot dienstverlening (dit kan ook verlopen via de telefoondienst)	-Wettelijke termijn van minimaal 7 jaar
Certificaatgegevens inclusief pasje op creditcardformaat*	-Voorletters en achternaam* -Geboorteplaats* -Geboortedatum* -Certificaatnummer -Uitvoeringsdatum training* -Verloopdatum certificaat -Resultaten van theorie- en praktijktesten*	-Zorgdragen dat herleidbaar is wie een betreffende training heeft gevolgd -Vastlegging van positieve of negatieve beoordeling van de kandidaat -Bewaken van geldigheid certificaat en tijdig informeren van opdrachtgever in relatie tot verloop van certificaten -Voldoen aan Arbowetgeving	-In verband met het kunnen tonen van een opleidingshistorie (ISZW) is er geen maximale bewaartermijn vastgesteld.
Rapportgegevens* & bedrijfshandboeken*	-Bedrijfsnaam -Vestigingsadres -Bedrijfssamenstelling -Postadres -Namen van geïnterviewde personen -Certificaatnummers en verloopdatum	-Zorgdragen dat rapportages zijn opgesteld op basis van feitelijke gegevens die verifieerbaar zijn door de klant of externe partijen die bedrijfscontroles uitvoeren zoals Inspectie SZW of certificerende instanties.	-Maximaal 10 jaar

Onderdeel	Gegevens	Doel	Bewaartermijn
Website*	-IP-adressen -Google Analytics -Naam, telefoonnummer en mailadres -Offertegegevens	-Ter verbetering van de website. -Beantwoorden van ingestuurde vragen -Opstellen van offertes -Abonneren op nieuwsbrief	-Maximaal 5 jaar
Projectmanagement* & Interimmanagement*	-Curriculum Vitae -Persoonsgegevens -Namen van medewerkers	-Detachering van veiligheidskundigen op projecten -Rapportages die een relatie hebben met project- of interim gerelateerde zaken (overlegvormen, onderzoeken en dergelijke)	-Deze wordt verwijderd indien beide partijen aangeven geen gebruik meer te willen maken van elkaars diensten.

** Deze gegevens kunnen worden gedeeld met derden ten behoeve van uitbesteedde activiteiten zoals het verzorgen van trainingen, laten toetsen van rapporten & bedrijfshandboeken en detacheringsklussen. Hiervoor zijn verwerkingsovereenkomsten aanwezig of deze zullen worden opgesteld indien deze niet aanwezig zijn.*

AVG-grondslagen

Binnen HESQ Support beroepen wij ons op drie AVG-grondslagen. Dit betreffen de volgende grondslagen:

- Toestemming
- Uitvoering van overeenkomst
- Nakomen wettelijke verplichting

Toestemming

Dit heeft betrekking op het verzamelen van data met betrekking tot de website en telefoondienst. Zonder juiste contactgegevens of onvolledige details is het voor ons niet mogelijk om een reactie te geven op eventuele vragen of prijsaanvragen. Hiervoor wordt wel om toestemming gevraagd en verwezen naar deze privacyverklaring die ook online is gepubliceerd.

Uitvoering van overeenkomst

Inspectie SZW, certificerende instanties en opdrachtgevers moeten kunnen verifiëren welk medewerkers trainingen hebben gevolgd. Dit is alleen te verifiëren door bepaalde documenten op te stellen en te bewaren zoals genoemd in de tabel op pagina 1 en 2. Ditzelfde geldt voor gegevens van rapportages zoals auditrapporten en Risico-Inventarisaties & -Evaluaties, ongevalsonderzoeken, VGM-projectplannen en dergelijke.

Nakomen wettelijke verplichting

Dit heeft met name betrekking op de belastingwet. In sommige gevallen heeft dit ook betrekking op trainingen omdat sommige trainingen wettelijk zijn vastgelegd in Arbowetgeving of onderliggende regelgeving. Dit heeft betrekking op bijvoorbeeld TCVT-hijstrainingen, maar ook trainingen die worden vermeld in door de Inspectie ISZW getoetste Arbocatalogi.

Indien u van mening bent dat u bepaalde gegevens niet hoeft te verstrekken kan dit leiden tot het niet (volledig) uitvoeren van de opdracht of taak. In een dergelijk geval kunt u hiervan melding maken bij de verwerkingsverantwoordelijke. Er wordt getracht een oplossing te vinden waar beide partijen zich in kunnen vinden. Deze communicatie zal schriftelijk plaatsvinden.

De heer K.J. Bolkenbaas is de verwerkingsverantwoordelijke.
Zijn contactgegevens zijn:

Adres Van Duivenvoordestraat 45
4926BT Lage Zwaluwe
Mail info@hesqsupport.nl
Tel 085 301 3010

Geautomatiseerde besluitvorming

Binnen HESQ Support vindt er geen geautomatiseerde besluitvorming plaats.

Verwerking

Verwerkingsverantwoordelijke

Binnen HESQ Support is de heer K.J. Bolkenbaas aangesteld als verwerkingsverantwoordelijke en tevens functionaris gegevensbescherming (FG).

Zijn contactgegevens zijn:

Adres Van Duivenvoordestraat 45
4926BT Lage Zwaluwe
Mail info@hesqsupport.nl
Tel 085 301 3010

Verwerkingsdoeleinden

HESQ Support is niet van plan uw persoonsgegevens door te geven aan partijen buiten de Europese Unie. Indien dit noodzakelijk is zal er eerst met u contact worden opgenomen om afspraken te maken omtrent het verzenden van relevante en strikt noodzakelijke persoonsgegevens. Deze communicatie zal schriftelijk plaatsvinden.

Per onderdeel is op pagina 1 en 2 in de tabel vermeld met welk doel persoonsgegevens worden verwerkt. In sommige gevallen worden persoonsgegevens doorgestuurd naar derden.

Verwerkings- en geheimhoudingsovereenkomst(en)

Hieronder wordt aangegeven welke gegevens wij kunnen doorsturen naar sub verwerker(s).

Onderdeel	Sub verwerker(s)	Doel
Facturatiegegevens	-Administratiekantoor -Microsoft One Drive	-Verwerken van in- en verkoopfacturen -Opstellen van jaarrekening
Certificaatgegevens inclusief pasje op creditcardformaat	-Opdrachtgevers -Collega opleiders -Inspectie SZW -Arbodienst -Microsoft One Drive	-Ter controle of juiste gegevens aanwezig zijn -Uitbesteedde trainingen of examens -In geval van een incident
Rapportgegevens & bedrijfshandboeken	-Opdrachtgevers -Certificerende instanties -Inspectie SZW -Microsoft One Drive	-Voor eigen gebruik -Vereist vanuit de norm waarvoor organisaties zich laten certificeren -In geval van een incident
Website	-Hosting -ICT-specialist -Telefoondienst	-Analyseren van gedrag bezoekers om website te optimaliseren -Opvangen telefoongesprekken en doorzetten van gespreksmemo's
Projectmanagement & Interimmanagement	-(Potentiële) opdrachtgevers en/of opdrachtnemers -Microsoft One Drive	-Beoordelen of de medewerker overeenkomt met het profiel van de potentiële opdrachtgever.

Met de betreffende partijen is of zal in de toekomst, indien hieraan nieuwe partijen worden toegevoegd, een samenwerkingsovereenkomst worden opgesteld waarin minimaal een verwerkings- en geheimhoudingsovereenkomst zijn opgenomen die voldoen aan de Algemene verordening gegevensbescherming (AVG).

Beleid ten behoeve van informatiebeveiliging

De verwerkingsverantwoordelijke heeft een inventarisatie gemaakt van mogelijke gebeurtenissen die kunnen leiden tot een datalek of beveiligingsincident. Op basis van deze inventarisatie zijn er zowel technische als organisatorische maatregelen genomen die de kans op een datalek of beveiligingsincident moeten minimaliseren.

Zowel de technische als organisatorische maatregelen vormen ons beleid ten behoeve van informatiebeveiliging.

Organisatorische maatregelen

- Verwerkings- en geheimhoudingsovereenkomsten met sub verwerkers;
- Oude documenten op een juiste wijze vernietigen;
- Ordentelijk werken, met name op externe locaties;
- Geen onnodige printopdrachten van persoonsgegevens;
- Wachtwoord van Microsoft One Drive en mail zijn direct te veranderen waardoor gebruiker geen toegang meer heeft tot alle persoonsgegevens of email;
- Niet onbeheerd achterlaten van laptop of telefoon (in kluisje of auto (overdag) of ’s avonds en ’s nachts in verblijflocatie);
- Documenten worden niet opgeslagen op harde schijf van de laptop;
- Beveiligde back-up van Microsoft One Drive.

Technische maatregelen

- Werken in de Cloud waardoor fysieke harde schijf niet kan worden ontvreemd
- Laptop en mobiele telefoon zijn alleen toegankelijk met wachtwoord
- Laptop en mobiel zijn bij verlies of diefstal direct te vergrendelen op afstand
- Werken met twee schermen waardoor er minder printactiviteiten van persoonsgegevens plaatsvinden;
- Plaatsen van rolluiken tegen inbraak op 1e verdieping;
- Alle deuren voorzien van automatische drie-punt sluiting;
- Gebruik van router met firewall en virusscanner op laptop

Protocol voor afhandeling datalekken en beveiligingsincidenten

Een datalek is de inbreuk op de beveiliging van persoonsgegevens. Een datalek betreft alle beveiligingsincidenten waardoor de bescherming van persoonsgegevens op enig moment is doorbroken waardoor de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking van persoonsgegevens.

Voorbeelden van een datalek zijn:

- een kwijtgeraakte USB-stick waar zich persoonsgegevens op bevinden;
- een gestolen werklaptop;
- een vastgestelde inbraak door een hacker;
- een besmetting met ransomware als er geen bruikbare back-up teruggezet kan worden
- papieren met persoonsgegevens belanden op straat
- een kwetsbaarheid in een applicatie waardoor persoonsgegevens gelekt worden

In beginsel moet ieder datalek aan de Autoriteit Persoonsgegevens worden gemeld. Alleen die datalekken waarbij het onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen zijn uitgezonderd van de meldplicht.

Wanneer wij hebben vastgesteld dat de inbreuk op de persoonsgegevens een hoog risico voor u als persoon inhoudt, zullen wij aan u mededelen dat er sprake is geweest van een inbreuk in verband met persoonsgegevens.

Wij hoeven u niet te infomeren wanneer:

- wij passende technische en organisatorische beschermingsmaatregelen hebben genomen, bijvoorbeeld in de vorm van versleuteling van de gegevens;
- wij achteraf maatregelen hebben genomen waarmee de vastgestelde risico's voor u zijn weggenomen;
- wij onevenredig veel inspanning moeten leveren. In dit geval kunnen wij volstaan met een openbare melding, bijvoorbeeld via een algemene mail of de website.

Verder zijn wij niet verplicht een datalek te melden in geval dit noodzakelijk is ter waarborging van:

- de nationale veiligheid;
- de landsverdediging;
- de openbare veiligheid;
- de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten, en de tenuitvoerlegging van straffen;
- andere belangrijke doelstellingen van algemeen belang van de Europese Unie of een lidstaat;
- de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;
- de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;
- een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt met de uitoefening van het openbaar gezag;
- de bescherming van de betrokkene of van de rechten en vrijheden van anderen;
- de inning van civielrechtelijke vorderingen.

Wij zullen onderstaande zaken aan u melden betreffende het datalek:

- een omschrijving van de aard van de inbreuk;
- de naam en contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van de inbreuk voor betrokkenen;
- de maatregelen die u heeft voorgesteld of genomen om de inbreuk aan te pakken, waaronder de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Wij zijn verplicht om een melding te doen bij de Autoriteit Persoonsgegevens. Op de volgende pagina wordt vermeld welke informatie wij dienen te verzamelen en overhandigen. Hiervoor kan mogelijk nog contact met u worden gezocht om te verifiëren of de melding op een juist wijze wordt ingediend.

Wij zullen de volgende gegevens bezorgen aan de Autoriteit Persoonsgegevens in geval van een datalek:

- de aard en omvang van de inbreuk;
- waar mogelijk de categorieën van betrokkenen, de persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
- de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- de maatregelen die u heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan

Bij het opstellen van dit protocol is gebruikt gemaakt van de Handleiding Algemene Verordening Gegevensbescherming die is opgesteld door het Ministerie van Justitie en Veiligheid

De verwerkingsverantwoordelijke, de heer K.J. Bolkenbaas, is verantwoordelijk voor de uitvoering van dit protocol. Zijn contactgegevens zijn:

Adres Van Duivenvoordestraat 45
4926BT Lage Zwaluwe
Mail info@hesqsupport.nl
Tel 085 301 3010

AVG-privacyrechten

U heeft het recht om uw persoonsgegevens in te zien, te corrigeren of te verwijderen. Daarnaast heeft u het recht om uw eventuele toestemming voor de gegevensverwerking in te trekken of bezwaar te maken tegen de verwerking van uw persoonsgegevens door HESQ Support en heeft u het recht op gegevensoverdraagbaarheid. Dat betekent dat u bij ons een verzoek kunt indienen om de persoonsgegevens die wij van u beschikken in een computerbestand naar u of een ander, door u genoemde organisatie, te sturen.

U kunt een verzoek tot inzage, correctie, verwijdering, gegevensoverdraging van uw persoonsgegevens of verzoek tot intrekking van uw toestemming of bezwaar op de verwerking van uw persoonsgegevens sturen naar de verwerkingsverantwoordelijke, de heer K.J. Bolkenbaas.
Zijn contactgegevens zijn:

Adres Van Duivenvoordestraat 45
4926BT Lage Zwaluwe
Mail info@hesqsupport.nl
Tel 085 301 3010

Daarnaast zijn wij verplicht u te wijzen op de klachtenprocedure van de Autoriteit Persoonsgegevens. Hier kunt u terecht indien u klachten heeft. Uiteraard hopen wij dat we onderling tot een oplossing kunnen komen wanneer u een klacht bij ons meld.

Wij zijn ervan overtuigd dat wij de juiste maatregelen hebben genomen om ervoor te zorgen dat uw gegevens en die van uw medewerkers op een juiste manier worden verwerkt en beschermd zijn tegen ongewilde gebeurtenissen.

Met vriendelijke groet,

K.J. Bolkenbaas
Founder | HESQ Expert | Lead Auditor