ISS beleid inzake bescherming Persoonsgegevens

BELEIDSVERKLARING

ISS levert wereldwijd diensten aan duizenden klanten en verwerkt daarbij, als één van de grootste werkgevers ter wereld, dagelijks Persoonsgegevens. Als een verantwoordelijk werkgever en dienstverlener neemt ISS de verplichting om gegevens overzichtelijk en veilig te verwerken zeer serieus. De bescherming van de integriteit van de Persoonsgegevens van onze werknemers, klanten en hun gebruikers is voor ISS van cruciaal belang.

Dit Beleid zet uiteen hoe ISS Persoonsgegevens verwerkt en welke maatregelen zij invoert om er zeker van te zijn dat gegevens van de klanten overzichtelijk en veilig worden verwerkt.

Het doel van dit Beleid is om jou inzage te geven in de verplichte minimumvereisten voor het verzamelen en verwerken van Persoonsgegevens binnen ISS. Dit Beleid bevat ook bepaalde voor jou verplichte procedures die ISS in staat stelt om aan de verplichtingen van toezichthouders te voldoen.

Naleving van dit Beleid is voor iedere werknemer binnen ISS die met Persoonsgegevens werkt, verplicht.

Dit document is een Nederlandse vertaling van de Data Protection Policy van de ISS Group en kan niet op al uw vragen antwoord geven en beoogt dit evenmin. In geval van vragen of suggesties ter verbetering van dit Beleid neem dan contact op met de afdeling Legal (tel: +31 30 242 43 61 of email legalteam.ISSNL@nl.issworld.com of Group Legal (tel.: +45 38 17 00 00 of email: dpo@group.issworld.com).

Hoogachtend,

Bjørn Raasteen
General Counsel van ISS Global A/S

Morten Lindegaard
Data Protection Officer
van ISS Global A/S

INHOUDSOPGAVE

Documentversie
Documentversie: Versie 1.0
Documentlocatie: Intranet

Laatst bijgewerkt: februari 2018
Goedgekeurd door: directie ISS Nederland
Verantwoordelijk voor onderhoud: Legal
Volgende evaluatie / bijwerking: na update Engelse versie

1 INTRODUCTIE

1.1 Fundamentele regels

ISS is als dienstverlener wereldwijd werkzaam voor haar klanten. Het is belangrijk voor ISS dat het gebruik van Persoonsgegevens in overeenstemming is met de hoogste wettelijke standaarden. ISS heeft er daarom voor gekozen om zich wereldwijd aan de beginselen van de EU gegevensbeschermingsregelgeving te houden, tenzij lokaal recht een hogere standaard voorschrijft.

Om de hoge standaard voor het verwerken van Persoonsgegevens te waarborgen houdt ISS zich aan de volgende basis principes:

(a) Integere en goede bedrijfsvoering voor de verwerking van Persoonsgegevens

ISS zorgt ervoor dat Persoonsgegevens veilig en overzichtelijk worden verwerkt in overeenstemming met algemeen aanvaardbare standaarden voor het verwerken van Persoonsgegevens. Met het oog op het doelbeginsel verwerkt ISS de gegevens niet buiten het specifieke doel waarvoor de Persoonsgegevens zijn verkregen.

(b) Persoonsgegevens uitsluitend verwerken voor een specifiek doeleinde

ISS verwerkt Persoonsgegevens uitsluitend voor doeleinde(n) waarvoor de gegevens oorspronkelijk zijn verzameld.

(c) Transparantie

ISS zorgt er voor dat bij het verzamelen van gegevens van betrokkenen zij de door de wet vereiste informatie ontvangen. Voorts hebben de betrokkenen en de klanten van ISS altijd het recht informatie op te vragen over de door ISS verzamelde Persoonsgegevens en hoe deze Persoonsgegevens worden verwerkt.

(d) Vertrouwelijkheid

Alle door ISS verwerkte Persoonsgegevens worden als vertrouwelijke informatie geclassificeerd. Om de vertrouwelijkheid van Persoonsgegevens te waarborgen zal ISS haar werknemers (i) instrueren hoe Persoonsgegevens kunnen worden verwerkt en (ii) bewust maken van de vertrouwelijke aard van Persoonsgegevens.

1.4 Definities gebruikt in dit Beleid

Betrokkene: De Betrokkene is een identificeerbaar natuurlijk persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator, zoals een naam, een identificatienummer, locatiegegevens, een online indicator of één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Binding Corporate Rules (BCR): Om de overdracht van Persoonsgegevens tussen onze entiteiten te waarborgen heeft ISS zich op wereldwijd niveau verbonden aan een set Binding Corporate Rules, welke goedgekeurd is door de Autoriteiten voor Gegevensbescherming in de Europese Unie. Een lijst met ISS-landen die de BCR hebben getekend is beschikbaar op https://dataprotection.group.issworld.com.

Country Management: Voor elk ISS-land, de Country Manager en alle managers die direct aan de Country Manager rapporteren, inclusief maar niet beperkt tot de Country Chief Financial Officer, Director People & Culture, Commercial Director, Director Corporate Affairs and the business segment Directors.

Data Map: Elk ISS-land of -entiteit is verantwoordelijk voor het bijhouden van een lijst van de te verwerken Persoonsgegevens, hoe en waar zij worden verwerkt en wie toegang tot deze Persoonsgegevens heeft. De lokale DPO onderhoudt de Data Map en rapporteert deze tweejaarlijks aan de Group DPO.

Data Protection Impact Assessment report of DPIA: Een privacy impact assessment is een instrument om van voorgenomen systemen en projecten welke Persoonsgegevens verwerkt, de privacy risico's van de gegevensverwerking voor Betrokkenen op een gestructureerde en gestandaardiseerde wijze in kaart te brengen en te beoordelen. De DPIA stelt uiteindelijk vast welke maatregelen de privacy risico's met betrekking tot dat systeem en/of project moet verkleinen tot acceptabel niveau.

EER: De Europese Economische Ruimte (EER) verenigt de EU-lidstaten en, IJsland, Liechtenstein en Noorwegen, in een interne markt die wordt beheerst door dezelfde basisregels. De EU-lidstaten zijn: België, Bulgarije, Cyprus, Duitsland, Estland, Finland, Frankrijk, Griekenland, Hongarije, Ierland, Italië, Kroatië, Letland, Litouwen, Luxemburg, Malta, Nederland, Oostenrijk, Polen, Portugal, Roemenië, Slowakije, Slovenië, Spanje, Tsjechië, Verenigd Koninkrijk en Zweden.

GDPR: De General Data Protection Regulation (GDPR), in Nederland ook wel Algemene Verordening Gegevensbescherming (AVG) genoemd, vormt de algemene verwijzing naar EU-verordening 2016/679, ter vervanging van de Europese Richtlijn Gegevensbescherming en de Wet Bescherming Persoonsgegevens in Nederland. De AVG werd op 27 april 2016 aangenomen en treedt op 25 mei 2018 in werking. Anders dan bij een richtlijn hoeft de AVG niet te worden omgezet in Nederlandse wetgeving. De AVG heeft rechtstreekse werking en is direct van toepassing.

Group DPO: De ISS Group Data Protection Officer. De Group DPO gaat de algehele wereldwijde naleving van regels voor gegevensbescherming na, geeft training aan Lokale DPO's en adviseert bij alle vragen met betrekking tot dit Beleid en de implementatie hiervan.

Informatiebeveiligingsbeleid: Het ISS Informatiebeveiligingsbeleid, inclusief al het sub-beleid. Dit beleid is beschikbaar op https://dataprotection.group.issworld.com.

ISS Groepsbeleid: Beleid en richtlijnen uitgevaardigd en regelmatig bijgewerkt door de ISS Group en beschikbaar op https://governance-policies.group.issworld.com.

Lokale DPO: In de meeste landen heeft het Country Management een lokale Data Protection Officer aangesteld (indien vereist op grond van de wet of het management) of een lokale privacy officer. Een lijst met Lokale DPO's is beschikbaar op https://dataprotection.group.issworld.com.

Persoonsgegevens: Alle informatie over een geïdentificeerde of een identificeerbare natuurlijk persoon ('Betrokkene').

Bijzondere Categorie van Persoonsgegevens: Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gezondheidsgegevens, gegevens met betrekking tot iemands seksueel gedrag of seksuele geaardheid, blijken.

In aanvulling op deze categorieën kunnen er aanvullende lokale vereisten bestaan voor bepaalde soorten gegevens die als een Bijzondere Categorie van Persoonsgegevens worden beschouwd. Als u twijfelt over dergelijke lokale vereisten, vraag dit dan na bij de Lokale DPO of de Group DPO. Voor Nederland geldt dat het BSN-nummer alleen mag worden verwerkt als er een wettelijke grondslag is.

Verantwoordelijke: Een natuurlijke persoon of rechtspersoon, overheidsinstantie, dienst of ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van Persoonsgegevens vaststelt. Bijvoorbeeld, ISS wordt normaliter beschouwd als de Verantwoordelijke voor de Persoonsgegevens van onze werknemers.

Verwerker: Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of ander orgaan die/dat ten behoeve van de Verantwoordelijke Persoonsgegevens verwerkt. Bijvoorbeeld, de leveranciers van ISS worden normaliter beschouwd als Verwerkers als zij Persoonsgegevens van werknemers van ISS verwerken. Indien ISS Persoonsgegevens van de werknemers van klanten verwerkt, dan is ISS de Verwerker.

Subverwerker: Een leverancier van de Verwerker, die (ook) toegang heeft tot de van de Verantwoordelijke ontvangen Persoonsgegevens.

Verwerkingsovereenkomst: Het verwerken van de gegevens door de Verwerker moet worden geregeld door een bindende overeenkomst tussen de Verantwoordelijke en de Verwerker. Deze overeenkomst moet de duur en het doeleinde van de verwerking, het type te verwerken Persoonsgegevens en de rechten en verplichtingen van de Verantwoordelijke bevatten. De Persoonsgegevens kunnen uitsluitend op gedocumenteerde instructie van de Verantwoordelijke worden verwerkt. De Verwerker is verplicht de Verantwoordelijke te informeren in geval deze van mening is dat een instructie van de Verantwoordelijke om informatie te verwerken in strijd met de AVG of andere toepasselijke lokale wetgeving is.

1.5 Vragen – Evaluatie van Beleid

Als u vragen over dit Beleid of over een bepaald onderwerp of een bepaalde transactie hebt, dient u deze te richten aan de Group DPO (Tel: +45 38 17 00 00 of email: dpo@group.issworld.com). In geval van twijfel altijd hulp vragen of verzoeken, voordat u verder gaat.

De Engelse versie van dit Beleid wordt, waar vereist en ten minste jaarlijks, door de EGM geëvalueerd.

2 BEGINSELEN VOOR GEGEVENSBESCHERMING

2.1 Naleving van toepasselijke gegevensbeschermingswetgeving

Om aan de voorgeschreven regels voor gegevensbescherming te voldoen moet ISS in staat zijn gedocumenteerd aan te tonen dat de volgende zes beginselen worden gerespecteerd.

2.1.1 Rechtmatigheid van gegevensbescherming

ISS Beleid

Als ISS Persoonsgegevens verzamelt of verwerkt, moet dit in overeenstemming zijn met de relevante wettelijke bepalingen.

Hoe wij dingen doen

ISS heeft processen en procedures ingevoerd om te waarborgen dat personeel van ISS dat Persoonsgegevens verwerkt, weet dat ISS uitsluitend gegevens mag verwerken als ISS daar een wettelijke grondslag voor heeft.

Bij het verwerken van Persoonsgegevens van onze klanten moet ISS er zeker van zijn dat (i) ISS schriftelijke instructies voor het verwerken van de Persoonsgegevens heeft ontvangen en (ii) Persoonsgegevens uitsluitend in overeenstemming met deze instructies worden verwerkt.

Minimumvereisten

Met betrekking tot de rechtmatigheid van de verwerking van Persoonsgegevens gelden de volgende minimumvereisten:

De verwerking van Persoonsgegevens is uitsluitend toegestaan als aan ten minste één van de volgende voorwaarden is voldaan:

i. de Betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
ii. de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de Betrokkene partij is, bijvoorbeeld een arbeidsovereenkomst;
iii. de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de Verantwoordelijke (ISS) rust.
iv. de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de Verantwoordelijke (ISS) of van een derde, tenzij de belangen of de grondrechten en de fundamentele vrijheden van de Betrokkene zwaarder wegen.
v. de verwerking wordt door ISS namens de klant op grond van een Verwerkingsovereenkomst uitgevoerd.

Beschikbare hulpmiddelen

Hulpmiddelen zijn in het Engels beschikbaar op https://dataprotection.group.issworld.com.
• Guideline on determining categories of Personal Data and applicable legal basis for processing
• ISS Data Processing Agreement (afdeling Legal heeft een Nederlandse versie beschikbaar)
• ISS Guidelines on third party Data Processing Agreements

2.1.2 Doeleinde van gegevensverwerking

ISS Beleid

ISS verwerkt geen Persoonsgegevens anders dan voor de doeleinden waarvoor de gegevens oorspronkelijk werden verzameld, tenzij de Betrokkenen hun toestemming hebben verleend of voor zover dit op grond van de wet is toegestaan.

Hoe wij dingen doen

ISS is verplicht het oorspronkelijke doeleinde (de oorspronkelijke doeleinden) van de gegevensverzameling bij het verder verwerken of gebruiken van Persoonsgegevens, te respecteren. Ook als de Persoonsgegevens van een andere ISS-entiteit zijn ontvangen. Het doeleinde van gegevensverwerking kan ISS uitsluitend wijzigen met toestemming van de Betrokkene of voor zover dit op grond van de wet is toegestaan.

Minimumvereisten

Met betrekking tot het doeleinde van de verwerking van Persoonsgegevens gelden de volgende minimum vereisten:

i. Iedere ISS-entiteit moet een lokale Data Map aanleggen en bijhouden. Deze Data Map moet beschikbaar zijn voor de Group DPO.
ii. Persoonsgegevens worden uitsluitend verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.
iii. Het doeleinde waarvoor Persoonsgegevens worden verwerkt, moet door ISS bij aanvang van de verzameling van de gegevens worden gedocumenteerd.
iv. In geen enkel geval worden Persoonsgegevens verwerkt op een wijze die niet verenigbaar is met de gerechtvaardigde doeleinden waarvoor de Persoonsgegevens worden verzameld.

Beschikbare hulpmiddelen

Hulpmiddelen zijn in het Engels beschikbaar op https://dataprotection.group.issworld.com .
• Methodology for Data Map and Risk Log
• Risk evaluation guideline
• Consent form

2.1.3 Transparantie in gegevensverwerking

ISS Beleid

ISS verwerkt Persoonsgegevens transparant en beantwoordt verzoeken van Betrokkenen om informatie.

Hoe wij dingen doen

Als ISS als Verantwoordelijke Persoonsgegevens verwerkt, zorgt ISS er voor dat Betrokkenen de informatie krijgen, zoals door de wet voorgeschreven. Als een Betrokkene hier om verzoekt, bevestigt ISS of zij Persoonsgegevens verwerkt en, indien dit het geval is, verstrekt ISS informatie omtrent de verwerkte Persoonsgegevens voor zover op grond van de wet is vereist.

ISS zorgt er voor dat Betrokkenen worden doorverwezen naar één contactpersoon die verantwoordelijk is voor het verstrekken van bovengenoemde informatie. De contactpersoon is de Lokale DPO of de Group DPO voor landen zonder een Lokale DPO.

Minimumvereisten

Met betrekking tot transparantie van de verwerking van Persoonsgegevens gelden de volgende minimumvereisten:

i. Elk ISS-entiteit zal Betrokkenen, klanten en lokale autoriteiten vanuit één enkel contactpunt informeren. Tevens kunnen zij hier informatie opvragen waartoe zij op grond van de wet gerechtigd zijn.

Beschikbare hulpmiddelen

Hulpmiddelen zijn in het Engels beschikbaar op https://dataprotection.group.issworld.com.
• Guideline on data protection information statements
• ISS information access request procedure

2.1.4 Gegevenskwaliteit en proportionaliteit

ISS Beleid

ISS waarborgt dat de Persoonsgegevens die door ISS als Verantwoordelijke worden verwerkt juist, toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is in verband met de doeleinden waarvoor de Persoonsgegevens worden verwerkt.

Hoe wij dingen doen

De verwerking van Persoonsgegevens door ISS wordt bepaald door het proportionaliteitsbeginsel. Dit betekent dat ISS Persoonsgegevens uitsluitend verzamelt, verwerkt en gebruikt voor zover dit vereist is voor het relevante doeleinde van de verwerking. Ondanks dat het voor ISS mogelijk kan zijn om meer Persoonsgegevens te verzamelen dan strikt noodzakelijk is voor het relevante doeleinde, zal ISS deze gegevens niet verzamelen en verwerken.

ISS kan Persoonsgegevens anonimiseren of pseudonimiseren, zodat deze gegevens niet ter zake dienend zijn voor gegevensbeschermingsdoeleinden.

ISS zorgt er voor dat Persoonsgegevens juist en actueel zijn. ISS neemt noodzakelijke maatregelen om zeker te stellen dat onjuiste of incomplete Persoonsgegevens worden gecorrigeerd, geblokkeerd of verwijderd.

Minimumvereisten

Met betrekking tot gegevenskwaliteit en proportionaliteit van de verwerking van Persoonsgegevens gelden de volgende minimumvereisten:

Beschikbare hulpmiddelen

i. ISS zorgt ervoor dat zij uitsluitend Persoonsgegevens verzamelt die relevant zijn voor het doeleinde van de verwerking en documenteert dit in de lokale Data Map.

ii. ISS verzamelt of verwerkt geen Persoonsgegevens als ISS weet of vermoedt dat de Persoonsgegevens niet juist zijn en richt een procedure in om zeker te stellen dat Persoonsgegevens worden bijgewerkt dan wel actueel zijn.

Hulpmiddelen zijn in het Engels beschikbaar op https://dataprotection.group.issworld.com.

- ISS Data Retention and Deletion Protocol (afdeling Legal Nederland heeft een Nederlandse versie beschikbaar).

2.1.5 Overdracht van persoonsgegevens en gebruik van Subverwerkers

ISS Beleid

Een kernaspect van het beschermen van Persoonsgegevens is waarborgen dat ISS een behoorlijk beschermingsniveau in acht neemt bij doorgifte van Persoonsgegevens tussen ISS-entiteiten dan wel van ISS naar derden. ISS zorgt er voor dat zij Persoonsgegevens uitsluitend tussen ISS-entiteiten of aan derden doorgeeft indien daarvoor een wettelijke basis voor overdracht bestaat

Hoe wij dingen doen

Overdracht van Persoonsgegevens tussen ISS-entiteiten

ISS heeft Binding Corporate Rules (BCR) ingevoerd die de doorgifte van Persoonsgegevens tussen ISS-entiteiten regelen. Overeenkomstig de BCR hebben alle ondertekende ISS-entiteiten zich verbonden om een adequate bescherming te waarborgen van Persoonsgegevens die zij ontvangen van andere ISS-entiteiten. Als ISS als Verwerker handelt, kan zij op grond van de BCR Persoonsgegevens aan een subverwerker van ISS doorgeven voor zover een ISS-entiteit de Verantwoordelijke is voor de door te geven Persoonsgegevens.

Doorgifte van Persoonsgegevens van ISS aan een derde binnen de EER

Bij doorgifte van Persoonsgegevens van ISS aan een derde, gevestigd in de EER of in Zwitserland, zal ISS zeker stellen dat partijen een Verwerkingsovereenkomst hebben gesloten en dat aan één van de volgende voorwaarden wordt voldaan:

(a) De ISS Modelverwerkingsovereenkomst is gebruikt tussen ISS en de ontvangende derde ; of

(b) De checklijst van de Verwerkingsovereenkomst is gevolgd en alle vereiste aangelegenheden zijn behandeld.

Doorgifte van Persoonsgegevens van ISS aan een derde buiten de EER

Bij doorgifte van Persoonsgegevens van ISS aan een derde, gevestigd buiten de EER, zal ISS zeker stellen dat aan één van de volgende voorwaarden is voldaan:

(a) EU-modelcontract (Standard Contractual Clauses for Data Processors 2010/87/EU of Standard Contractual Clauses between Data Controllers 2001/497/EG of 2004/915/EG) is tussen ISS en de ontvangende derde gesloten; of

(b) De doorgifte is op grond van het toepasselijk recht toegestaan.

Gebruik van Verwerker en/of Subverwerker

Als ISS, handelend als Verantwoordelijke of Verwerker, een derde aanstelt voor het verwerken van Persoonsgegevens, draagt ISS er voor dat de volgende vereisten worden gerespecteerd:

(a) de Verwerker is zorgvuldig beoordeeld en geselecteerd door ISS op basis van de capaciteit van de Verwerker om de implementatie en het onderhoud van noodzakelijke technische en organisatorische beveiligingsmaatregelen met betrekking tot gegevensverwerking te waarborgen;

(b) ISS waarborgt en controleert regelmatig dat de Verwerker de overeengekomen technische en organisatorische beveiligingsmaatregelen volledig blijft naleven;

(c) ISS waarborgt dat de uitvoering van opgedragen gegevensverwerking in een schriftelijke Verwerkingsovereenkomst is geregeld waarin de rechten en de verplichtingen van de Verwerker duidelijk zijn gedefinieerd; en

(d) ISS waarborgt dat de Verwerker contractueel is gebonden om de van of namens ISS ontvangen Persoonsgegevens uitsluitend in overeenstemming met de overeenkomst en in overeenstemming met de instructies van ISS te verwerken.

Minimumvereisten

Met betrekking tot doorgifte van Persoonsgegevens en gebruik van subverwerkers voor verwerking van Persoonsgegevens gelden de volgende minimumvereisten:

i. Doorgifte van Persoonsgegevens tussen ISS-entiteiten vindt uitsluitend plaats als beide entiteiten de BCR hebben getekend of als het EU-modelcontract tussen de entiteiten is gesloten.

ii. Doorgifte van Persoonsgegevens van ISS aan een derde is uitsluitend toegestaan als de doorgifte voor gerechtvaardigde doeleinden in overeenstemming is met de wet en met inachtneming van contractuele beperkingen.

iii. Als ISS een derde inhuurt die namens ISS Persoonsgegevens verwerkt, moet tussen ISS en de derde een Verwerkingsovereenkomst worden gesloten. Doorgifte van Persoonsgegevens van ISS-entiteiten binnen de EER aan een derde, gevestigd buiten de EER, vindt uitsluitend plaats vinden als voor het uitvoeren van de doorgifte het modelcontract tussen partijen is gesloten.

iv. Alle bovenstaande doorgiften van Persoonsgegevens moeten in de lokale Data Map worden gedocumenteerd.

Beschikbare hulpmiddelen

Hulpmiddelen zijn in het Engels beschikbaar op https://dataprotection.group.issworld.com.

- Guideline on use of Data Processors
- ISS Data Processor Agreement (afd. Legal NL heeft een Nederlandse versie beschikbaar).
- Guideline on use of data transfer agreement
- EU Standard contractual clausus

Lijst met ISS-landen die de BCR hebben getekend

2.1.6 Bijzondere Categorieën van Persoonsgegevens

ISS Beleid

Bij het verwerken van Bijzondere Categorieën van Persoonsgegevens, zoals strafrechtelijke gegevens, persoonlijkheidstesten, gezondheidsgegevens en werk gerelateerde incidenten moeten specifieke voorzorgsmaatregelen worden getroffen.

Hoe wij dingen doen

Als ISS Bijzondere Categorieën van Persoonsgegevens moet verwerken, dient ISS hiervoor de uitdrukkelijke toestemming van de Betrokkene te krijgen, tenzij verwerking uitdrukkelijk is toegestaan op basis van de geldende wetgeving.

De Lokale DPO of Group DPO moet altijd worden geraadpleegd voordat ISS Bijzondere Categorieën van Persoonsgegevens gaat verwerken en deze verwerking moet in de lokale Data Map worden vastgelegd.

Indien ISS beoordeelt dat de verwerking van Bijzondere Categorieën van Persoonsgegevens een hoog risico voor de Betrokkenen met zich meebrengt, dan moet

een Data Protection Impact Assessment rapportage (DPIA) worden uitgevoerd.

Minimumvereisten

Met betrekking tot de Bijzondere Categorieën van Persoonsgegevens zijn de volgende minimumvereisten van toepassing:

i. Beoordeel voor het verzamelen en verwerken van Persoonsgegevens altijd of Bijzondere Categorieën van Persoonsgegevens hier onderdeel van zijn.
ii. Als ISS Bijzondere Categorieën van Persoonsgegevens verzamelt en verwerkt, moet de Lokale DPO of de Group DPO worden geraadpleegd ter beoordeling van het noodzakelijke instemmingsniveau, informatievereisten en het risico voor de Betrokkenen moet zorgvuldig in overweging worden genomen.
iii. Elke Verwerking van Bijzondere Categorieën van Persoonsgegevens moet ISS onmiddellijk in de lokale Data Map vastleggen.

Beschikbare hulpmiddelen

Hulpmiddelen zijn in het Engels beschikbaar op https://dataprotection.group.issworld.com.

• Guidelines on determining categories of Personal Data and applicable legal basis for processing

• DPIA guideline and template

3 GEGEVENS-BEVEILIGING

3.1 ISS Beleid

ISS waarborgt dat de noodzakelijke technische en organisatorische beveiligingsmaatregelen zijn ingericht ter bescherming van Persoonsgegevens tegen onopzettelijke of onrechtmatige vernietiging, verlies of wijziging, ongeautoriseerde openbaarmaking, misbruik of anderszins verwerking in strijd met de wet.

Rekening houdend met de implementatiekosten zullen deze maatregelen een beveiligingsniveau garanderen dat met het oog op de risico's, verbonden aan de verwerking en de aard van de te beschermen Persoonsgegevens, passend is. Bijzondere Categorieën Persoonsgegevens zijn aan bijzondere beveiligings- en beschermingsmaatregelen onderhevig.

3.2 Hoe wij dingen doen

Om aan deze vereisten te voldoen heeft ISS een Informatiebeveiligingsbeleid opgesteld, een IT-beveiligingsorganisatie ingericht en informatiebeveiliging in de processen van de ISS-organisatie geïntegreerd.

Uitsluitend personeel dat is geautoriseerd en speciaal getraind in naleving van informatiebeveiligingsvereisten, is toegestaan Persoonsgegevens te verzamelen, te verwerken of te gebruiken. Toegangsautorisatie van de individuele werknemer wordt beperkt overeenkomstig de aard en omvang van het specifieke werkgebied van de werknemer. Het is de werknemer verboden Persoonsgegevens voor privé-doeleinden te gebruiken en over te dragen of anderszins beschikbaar te stellen aan ongeautoriseerde personen. Onder ongeautoriseerde personen vallen in dit verband, bijvoorbeeld overige ISS-werknemers voor zover zij de Persoonsgegevens niet voor voltooiing van hun specifieke taken nodig hebben. De geheimhoudingsverplichting duurt ook na het einde van het dienstverband van de werknemer in kwestie voort.

De specifieke maatregelen om de informatiebeveiliging van Persoonsgegevens te waarborgen omvatten toegangscontroles, systeemtoegangscontroles, gegevenstoegangscontroles, overdrachtscontroles, invoercontroles, taakcontroles, beschikbaarheidscontroles en functiescheidingsmaatregelen.

Alle computers en mobiele apparatuur zijn beschermd met een wachtwoord / code. Het ISS interne netwerk heeft een firewallsysteem ter bescherming van interne bedrijfsdata tegen ongeautoriseerde externe toegang. Verzending van Persoonsgegevens binnen het eigen bedrijfsnetwerk is versleuteld, voor zover de aard en het beoogde doeleinde van de Persoonsgegevens dit vereist.

3.3 Minimumvereisten

Met betrekking tot de beveiliging van de verwerking van Persoonsgegevens zijn de volgende **minimumvereisten** van toepassing:

i. ISS verwerkt Persoonsgegevens uitsluitend in overeenstemming met het ISS Informatiebeveiligingsbeleid.

ii. Elk ISS-entiteit heeft een lokale contactpersoon aangesteld die verantwoordelijk is voor de implementatie en naleving van het ISS Beleid inzake Informatiebeveiliging.

3.4 Beschikbare hulpmiddelen

Hulpmiddelen zijn in het Engels beschikbaar op https://dataprotection.group.issworld.com.
• ISS Information Security Policy
• ISS Security Documentation Protocol
• ISS Data Retention and Deletion Protocol

4 Datalek

4.1 ISS Beleid

In geval de beveiliging van de verwerking van Persoonsgegevens is gecompromitteerd of waarschijnlijk is gecompromitteerd of als er anderszins sprake is van een ongeautoriseerde of onopzettelijke openbaarmaking van of toegang tot Persoonsgegevens dan moet de Lokale DPO of de Group DPO onmiddellijk worden geïnformeerd.

ISS heeft een specifiek protocol, het Datalek Protocol (Data Breach Protocol). Dit protocol legt uit hoe ISS een datalek behandelt om nadelige gevolgen voor Betrokkenen, onze klanten en onze onderneming te beperken. Dit alles om aan de van toepassing zijnde wetgeving en/of onze contractuele verplichtingen ten opzichte van onze klanten te voldoen.

4.2 Hoe wij dingen doen

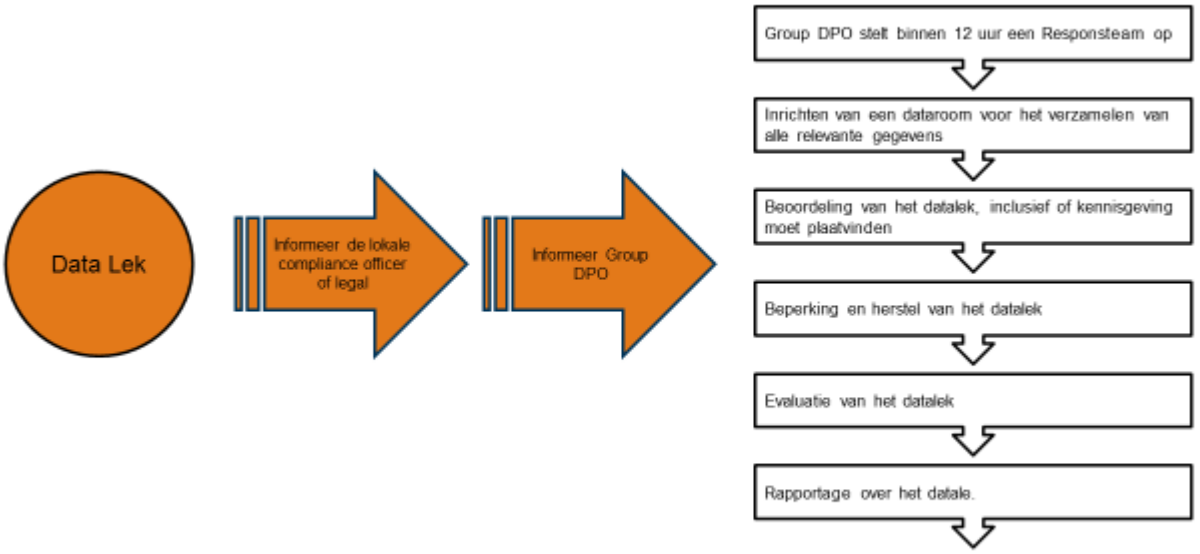
Om bewustzijn te creëren en onze werknemers te trainen in het identificeren en melden van datalekken in de informatiebeveiliging heeft ISS een trainingsmodule in datalekken in informatiebeveiliging opgezet. Deze trainingsmodule is beschikbaar via het ISS e-learning tool (MyLearning@ISS). Voor meer informatie over training en bewustmaking wordt naar hoofdstuk 5 van dit Beleid verwezen.

Als een werknemer van ISS ontdekt of een vermoeden heeft dat een ongeautoriseerde openbaarmaking van Persoonsgegevens of in geval de beveiliging aangaande Persoonsgegevens is aangetast of waarschijnlijk is aangetast, bijvoorbeeld vanwege een beveiligingslek, moet hij/zij direct contact opnemen met de Groep DPO en een Lokale DPO.

Het Datalek formulier verschaft de volgende informatie:

(a) welke ISS-entiteit wordt met het datalek geconfronteerd;
(b) samenvatting van het incident dat tot het datalek heeft geleid;
(c) datum en tijd van het datalek;
(d) het soort Persoonsgegevens dat is aangetast; en
(e) het aantal Betrokkenen waarop het datalek betrekking heeft.

Na ontvangst van de informatie omtrent een datalek zal de Group DPO er voor zorg dragen dat het volgende proces wordt gevolgd:



1

Om te waarborgen dat relevante functies binnen iedere ISS-entiteit de noodzakelijke kennis en ervaring hebben om adequaat op een datalek te reageren zal de Lokale DPO ten minste tweejaarlijks een datalekoefening met de Group DPO coördineren.

4.3 Minimumvereisten

Met betrekking tot datalekken zijn de volgende **minimumvereisten** van toepassing:

4.4 Beschikbare hulpmiddelen

i. Alle managers van Corporate Systems, People & Culture en Legal moeten de online trainingsmodule inzake datalekken (Module 2) hebben afgerond.
ii. Het Datalek Beleid inclusief bijlage 2 (contactgegevens) moet lokaal aan alle leden van Corporate Systems, People & Culture en Legal ter beschikking staan.
iii. De Lokale DPO zal ten minste tweejaarlijks een datalekoefening houden en daarover rapporteren.

Hulpmiddelen zijn in het Engels beschikbaar op https://dataprotection.group.issworld.com.
• The Data Protection Breach Protocol
• The Data Protection Breach Form
• Education module 2 (Data Protection Breach)
• Bijlage 1 van het 'Data Protection Breach Protocol' bevat de contactgegevens van alle ISS-functionarissen en -managers voor gegevensbescherming

5 TRAINING & BEWUSTMAKING

5.1 ISS Beleid

Als onderdeel van het ISS 'data protection compliance program' en als onderdeel van de implementatie van Binding Corporate Rules heeft ISS een trainingsprogramma voor ISS-managers en relevante werknemers opgezet.

Als onderdeel van de verplichtingen van ISS (juridisch en contractueel) om gegevensbeschermingstraining van werknemers te documenteren zal ISS de e-learningtool (MyLearning@ISS) gebruiken, die in ieder land beschikbaar is.

5.2 Hoe wij dingen doen

Het trainingsprogramma bestaat uit twee hoofdonderdelen, namelijk (i) Groep brede bewustmakingstraining (trainingsmodule 1 en 2) en (ii) individuele training met aandacht voor geselecteerde functies binnen ISS, zoals People & Culture , Procurement, Legal, Corporate Systems, Operatie, Sales en Finance.

De Group DPO onderhoudt en update het trainingsmateriaal.

5.3 Minimumvereisten

Met betrekking tot training en bewustmaking zijn de volgende **minimumvereisten** van toepassing:

i. Het Country Management binnen ISS-entiteiten die de BCR hebben getekend, moeten hebben deelgenomen aan trainingsmodules 1 en 2 en deze met succes hebben voltooid.
ii. De Group DPO en alle Lokale DPO moeten jaarlijks aan alle trainingsmodules deelnemen en met succes voltooien.

5.4 Beschikbare hulpmiddelen

Hulpmiddelen in het Engels zijn beschikbaar op https://dataprotection.group.issworld.com.
- Training module 1 – General Awareness
- Training module 2 – Data Breach

6 TOEZICHT EN AUDIT

6.1 ISS Beleid

De beginselen van gegevensbescherming van dit Beleid vormen een waardevolle bijdrage aan het verstandig en betrouwbaar uitoefenen van onze onderneming. Zij staan echter niet op zichzelf. Toezicht en audits inzake naleving van dit Beleid zijn belangrijk en noodzakelijk om verantwoording te documenteren en te waarborgen dat eventuele gaten worden gesignaleerd en op juiste wijze opgevolgd.

6.2 Hoe wij dingen doen

Implementatie en uitvoering van processen en procedures ter zekerstelling van naleving van de vereisten voor gegevensbescherming vindt dusdanig plaats dat toezicht en audits correct kunnen worden uitgevoerd. Dit betekent dat ISS de processen en procedures met betrekking tot de verwerking van Persoonsgegevens documenteert en wijzigingen in de processen en procedures in de lokale Data Map bijwerkt.

6.2.1 Interne audit

De Group DPO ziet toe op de interne auditwerkzaamheden, uitgevoerd door de Group Interne Audit, en adviseert om te waarborgen dat de auditwerkzaamheden de verwerking van Persoonsgegevens van ISS afdekken, inclusief methoden ter zekerstelling dat correctieve en preventieve acties zullen worden genomen.

ISS-entiteiten worden op regelmatige basis geaudit en een dergelijke audit omvat een audit inzake naleving van toepasselijke gegevensbeschermingswetgeving en dit Beleid. De audit wordt uitgevoerd door Group Interne Audit, andere interne specialisten of externe auditors.

De Group DPO is verantwoordelijk voor het onder de aandacht van de Chief Financial Officer en de Group General Counsel brengen van onregelmatigheden in het resultaat van een audit. Daarnaast zorgen zij er voor dat zo spoedig als redelijkerwijs mogelijk de onregelmatigheden worden opgelost.

6.2.2 Audit van ISS op verzoek van een klant

Klanten van ISS kunnen overeenkomstig de wet of een overeenkomst tussen partijen gerechtigd zijn een audit uit te voeren of een audit te verzoeken van een ISS-entiteit die namens de klant Persoonsgegevens verwerkt.

ISS zal haar klanten bij het uitvoeren van audits assisteren om zeker te stellen dat klanten van ISS er vertrouwen in hebben dat ISS de gegevensbeschermingswetgeving en overeengekomen contractuele verplichtingen nakomt.

6.2.3 Audit door ISS van leveranciers

Ter zekerstelling van naleving van de gegevensbeschermingswetgeving zal ISS regelmatig de verwerking van Persoonsgegevens namens ISS door haar leveranciers auditen. Audits kunnen fysiek op locatie bij de leveranciers worden uitgevoerd dan wel door het reviewen van auditrapporten van onafhankelijke derden.

6.3 Minimumvereisten

Met betrekking tot toezicht en audit zijn de volgende **minimumvereisten** van toepassing:

i. Country Management moet zeker stellen dat processen en procedures met betrekking tot de verwerking van Persoonsgegevens in de lokale Data Map zijn gedocumenteerd.
ii. Alle wijzigingen in de processen en procedures met betrekking tot de verwerking van Persoonsgegevens moet ISS regelmatig in de lokale Data Map bijwerken.
iii. De door ISS Group Interne audit uitgevoerde reguliere audit van ISS-entiteiten moet een audit van naleving van gegevensbescherming omvatten.
iv. De Group DPO moet het resultaat van gegevensbeschermingsaudits evalueren en aangelegenheden betreffende niet naleving onder de aandacht van de Chief Financial Officer en de Group Legal Counsel brengen.
v. ISS moet haar voorkeursleveranciers regelmatig auditen.

6.4 Beschikbare hulpmiddelen

Hulpmiddelen zijn in het Engels beschikbaar op https://dataprotection.group.issworld.com.

- The DPO check list
- ISS Audit Plan Protocol

Eerlijkheid

Wij respecteren

Ondernemerschap

Wij ondernemen actie

De ISS waarden

Verantwoordelijkheid

Wij zorgen

Kwaliteit

Wij leveren

ISS heeft een Klokkenluidersbeleid opgesteld om werknemers van ISS, zakenpartners en andere belanghebbenden de mogelijkheid te geven ernstige incidenten of misstanden op een vertrouwelijke manier te melden.

Een handleiding voor Klokkenluiders is beschikbaar op http://www.nl.issworld.com/verantwoordelijkheid/klokkenluidersregeling/handleiding-voor-klokkenluiders. Deze handleiding helpt u om te beoordelen of de kwestie (a) lokaal moet worden gemeld bij uw leidinggevende, manager, manager People & Culture, afdeling Legal of Chief Financial Officer of (b) moet worden gemeld aan Group Internal Audit in Kopenhagen, Denemarken, via een beveiligd meldingssysteem dat beschikbaar is op de site van ISS: http://www.nl.issworld.com/klokkenluidersregeling of via een telefonische hotline: + 44 20 36 30 17 01.

U kunt ook direct contact opnemen met:
Dan Otzen, hoofd van Group Internal Audit
ISS World Services A/S
Buddingevej 197, DK-2860 Soborg, Denmark
E-mail: Dan.Otzen@gruoup.issworld.com
Telefoonnummer: +45 38 17 68 00

Alle meldingen worden vertrouwelijk behandeld overeenkomstig het Klokkenluidersbeleid