

PERSOONSgegevensBELEID

Dit document beschrijft hoe Quaestor de bescherming van Persoonsgegevens verzekert bij het Verwerken ervan.

<p><u>Onderwerp:</u> Persoonsgegevens</p> <p><u>Laatste update:</u> 5/09/2023</p>	<p><u>Validering:</u> Raad van Bestuur op 11/09/2023</p> <p><u>Verantwoordelijke:</u> –raad van bestuur</p>
<p><u>Verbonden beleidslijnen – en procedures</u></p> <p><u>Onderstaande beleidslijn dient samen gelezen te worden met de hiernaast vernoemde beleidslijnen- en procedures.</u></p>	<ul style="list-style-type: none"> - Gegevensbewaringsbeleid - Informatiebeveiligingsbeleid - Register Verwerkingsactiviteiten - Register Datalekken - Register inzake Verzoeken voor de Uitoefening van Rechten

Inhoudstafel

I.	Introductie.....	4
II.	Definities	4
III.	Toepassingsgebied	6
IV.	Juridische bepalingen	7
V.	Rollen en verantwoordelijkheden.....	7
VI.	Implementatie.....	8
	1. Algemene verplichtingen	8
	2. Welke gegevens worden verwerkt.....	9
	3. Basisbeginselen van gegevensbescherming	9
	a. Rechtmatigheid, behoorlijkheid en transparantie	9
	b. Doelbinding	10
	c. Minimale gegevensverwerking.....	10
	d. Juistheid	10
	e. Opslagbeperking.....	10
	f. Integriteit en vertrouwelijkheid.....	10
	g. Doorgeven van Persoonsgegevens	11
	h. Verantwoordingsplicht.....	11
	i. Bijzondere aandacht bij het Verwerken van de gegevens buiten de EU	11
	4. Rechten van de Betrokkene	12
	a. Uitoefening van de rechten.....	12
	b. Recht op informatie en transparantie	12
	c. Recht van inzage.....	13
	d. Recht op rectificatie	13
	e. Recht op verwijdering van de Persoonsgegevens (“recht op vergetelheid”).....	13
	f. Recht op beperking van de Verwerking.....	14
	g. Recht op overdraagbaarheid.....	14
	h. Recht van bezwaar	14
	i. Recht om niet aan geautomatiseerde besluitvorming te worden onderworpen.....	15
	j. Recht op facilitering van de uitoefening van deze rechten	15
	5. Maatregelen om de naleving van de GDPR-verplichtingen te garanderen.....	15
	6. Verwerking van bepaalde categorieën van Persoonsgegevens.....	16
	a. Gevoelige gegevens.....	17
	b. Strafrechtelijke veroordelingen en feiten.....	17

c. Kinderen.....	17
7. Melding en registratie van inbreuken (datalekken).....	18
a. Interne melding	18
b. Melding aan de Betrokkene	18
c. Melding aan de GBA	19
d. Registratie van inbreuken	19
VII. Administratie	20
Bijlage A. Informatie te verstrekken aan de Betrokkene	21
Bijlage B. Informatie waartoe de Betrokkene inzage kan krijgen.....	23
Bijlage C. Richtlijnen informatieveiligheid	24
Bijlage D. Melding datalek aan de Betrokkene	25

Persoonsgegevensbeleid Quaestor

I. Introductie

Quaestor Vermogensbeheer NV (hierna: "Quaestor") is een beheervenootschap van niet-publieke alternatieve instellingen voor collectieve belegging ("AICB's") in de zin van artikel 3,12° van de Wet van 19 april 2014 betreffende de alternatieve instellingen voor collectieve belegging en hun beheerders (hierna de "AICB-wet") met een bijkomende toelating om bepaalde beleggingsdiensten zoals vermogensbeheer, beleggingsadvies en het ontvangen en doorgeven van orders in de zin van artikel 2 van de wet van 25 oktober 2016 betreffende de toegang tot het beleggingsdienstenbedrijf en betreffende het statuut van en het toezicht op de vennootschappen voor vermogensbeheer en beleggingsadvies (hierna de "VVB-wet") te verstrekken.¹

II. Definities

"Betrokkene"²: geïdentificeerde of identificeerbare natuurlijke persoon.

"Bijzondere categorieën van Persoonsgegevens ("Gevoelige gegevens")"³:

- Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken;
- Genetische gegevens, Biometrische gegevens met het oog op de unieke identificatie van een persoon, of Gegevens over gezondheid;
- Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

"Biometrische gegevens"⁴: Persoonsgegevens die het resultaat zijn van een specifieke technische Verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens.

"Compliance functie": een onafhankelijke controlefunctie, uitgeoefend door een Medewerker met de vereiste kennis en ervaring (Compliance Officer), gericht op de naleving van de regels met betrekking tot de integriteit van de activiteiten en het beheer van het compliance risico bij Quaestor.

"Data Protection Impact Assessment" ("DPIA")⁵: een beoordeling van het effect van de beoogde Verwerkingsactiviteiten op de bescherming van Persoonsgegevens.

"Data Protection Officer" ("DPO"): Tom Decloedt

¹ Op het vlak van het beheer van AICB's legt Quaestor zich voornamelijk toe op het beheer van private equity en durfkapitaalfondsen, veelal gestructureerd als een "private privak" (d.w.z. een private AICB gereguleerd door het Koninklijk Besluit van 23 mei 2007 met betrekking tot de "private privak" met een vast aantal rechten van deelneming, statutair geregeld en met als uitsluitend doel het beleggen in financiële instrumenten uitgegeven door niet-beursgenoteerde ondernemingen). Beleggingen in een private privak zijn uitsluitend voorbehouden aan Private beleggers.

² In overeenstemming met art. 4, 1) GDPR

³ In overeenstemming met art. 9 GDPR

⁴ In overeenstemming met art. 4, 14 GDPR

⁵ In overeenstemming met art. 35 GDPR

“**Effectieve Leiding**”⁶: de groep van personen binnen Quaestor, al dan niet bestuurders, van wie de functie binnen de instelling inhoudt dat zij op het hoogste niveau een rechtstreekse en doorslaggevende invloed uitoefenen op de leiding van de ondernemingsactiviteit.

“**GBA**”⁷: de Belgische gegevensbeschermingsautoriteit

“**Gegevens over gezondheid**”⁸: Persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.

“**Genetische gegevens**”⁹: Persoonsgegevens die verband houden met de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon.

“**Kind**”¹⁰: elke natuurlijke persoon jonger dan 13 jaar.

“**Medewerker**”:

- Een directeur, een vennoot of daarmee gelijk te stellen persoon, een bestuurder of een verbonden agent van Quaestor;
- Een werknemer van Quaestor of van een verbonden agent van Quaestor, alsook enigerlei andere natuurlijke persoon wiens diensten ter beschikking en onder de zeggenschap staan van Quaestor of een verbonden agent en die betrokken is bij het verrichten door Quaestor van haar beleggings- of beheerdiensten;
- Een natuurlijke persoon die uit hoofde van een uitbestedingsovereenkomst met het oog op het verrichten door Quaestor van beleggings- of beheerdiensten rechtstreeks betrokken is bij het verrichten van diensten ten behoeve van Quaestor of haar verbonden agent.

“**Persoonsgegevens**”¹¹: Gegevens zijn Persoonsgegevens indien ze betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon (i.e. de Betrokkene). Een natuurlijk persoon is identificeerbaar wanneer deze direct of indirect kan worden geïdentificeerd aan de hand van een identicator (bijv. naam, identificatienummer, locatiegegevens, online identicator) of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

“**Private belegger**”¹²: beleggers die, in het kader van een aanbieding die geen openbaar karakter heeft in de zin van de AICB-wet, voor eigen rekening ingaan of zijn ingegaan op de volgende aanbiedingen van effecten uitgegeven door een “private privak”

- aanbiedingen van effecten die een totale tegenwaarde van ten minste 25.000 euro per belegger en per categorie effecten vereisen;
- aanbiedingen met een nominale waarde per eenheid van ten minste 25.000 euro.

⁶ <https://www.fsma.be/nl/fag/a8-wat-effectieve-leiding>

⁷ <https://gegevensbeschermingsautoriteit.be/professioneel>

⁸ In overeenstemming met art. 4, 15) GDPR

⁹ In overeenstemming met art. 4, 13) GDPR

¹⁰ In overeenstemming met art. 7 Privacywet

¹¹ In overeenstemming met art. 4, 1) GDPR

¹² In overeenstemming met artikel 2,1° KB Private Privaks

“Profilering”¹³: Elke vorm van geautomatiseerde Verwerking van Persoonsgegevens waarbij aan de hand van Persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

“Pseudonimisering”¹⁴: het Verwerken van Persoonsgegevens op zodanige wijze dat de Persoonsgegevens niet meer aan een specifieke Betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de Persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

“Verantwoordelijke voor de Klantenrelaties”: Philippe Vanmarcke

“Verwerken of Verwerking”¹⁵: een bewerking of een geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

“Verwerker”¹⁶: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens verwerkt.

“Verwerkingsverantwoordelijke”¹⁷: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de Verwerking van Persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze Verwerking in het Unierecht of het nationaal recht worden vastgesteld, kan daarin worden bepaald wie de Verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.

III. Toepassingsgebied

Dit Beleid is opgesteld en dient te worden nageleefd om de bescherming van alle natuurlijke personen wiens Persoonsgegevens worden Verwerkt door Quaestor te verzekeren. Bijgevolg dient dit Beleid te worden nageleefd door elke Medewerker. Aangezien Quaestor Persoonsgegevens verwerkt binnen de Europese Unie, is dit Beleid van toepassing op elke Verwerking van Persoonsgegevens door Quaestor, ongeacht of Quaestor optreedt als Verwerkingsverantwoordelijke of als Verwerker. De regelgeving rond de Verwerking van Persoonsgegevens heeft alleen betrekking op natuurlijke personen en op

¹³ In overeenstemming met art. 4, 4) GDPR

¹⁴ In overeenstemming met artikel 4, 5) GDPR

¹⁵ In overeenstemming met art. 4, 2) GDPR

¹⁶ In overeenstemming met art. 4, 8) GDPR

¹⁷ In overeenstemming met art. 4, 7) GDPR

personen die een rechtspersoon vertegenwoordigen zoals een bedrijf, een gemeente of een vereniging.

IV. Juridische bepalingen

Dit Persoonsgegevensbeleid werd opgesteld ingevolge en in overeenstemming met de toepasselijke bepalingen op Belgisch en Europees niveau:

Op Europees niveau:

- Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de Verwerking van Persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (hierna: “GDPR”);
- EDPB Guidelines¹⁸;
- Article 29 Working Party Guidelines¹⁹.

Op nationaal niveau:

- Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de Verwerking van Persoonsgegevens (hierna: “Privacywet”).

V. Rollen en verantwoordelijkheden

• Medewerkers:

o Elke Medewerker handelt in overeenstemming met dit Beleid, de procedures en de controles opgesteld door de Effectieve Leiding;

o Elke Medewerker is verantwoordelijk om zijn/ haar handelingen te controleren en risico's inzake Verwerking van Persoonsgegevens te identificeren en passende maatregelen te nemen.

• Afdelingshoofd:

o Elk afdelingshoofd garandeert de naleving van de verplichtingen inzake de Verwerking van Persoonsgegevens binnen zijn/haar afdeling.

• De raad van bestuur:

o De raad van bestuur keurt de maatregelen inzake gegevensbescherming goed;

o De raad van bestuur keurt significante wijzigingen aan het Persoonsgegevensbeleid goed.

• De Effectieve Leiding:

¹⁸ https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_en

¹⁹ <https://ec.europa.eu/newsroom/article29/items/itemType/1360>

- o De Effectieve Leiding staat in voor de implementatie en navolging van de regels inzake gegevensbescherming in Quaestor;
 - o De Effectieve Leiding stelt een DPO aan binnen Compliance;
 - o Zij betreft de DPO bij alle relevante zaken inzake gegevensbescherming.
- DPO:
 - o De DPO is het aanspreekpunt voor alle personen voor vragen inzake gegevensbescherming;
 - o De DPO voert een periodieke controle uit of Quaestor handelt in lijn met de GDPR;
 - o De DPO staat in voor het informeren en adviseren van alle Medewerkers inzake alles over gegevensbescherming;
 - o De DPO rapporteert minstens jaarlijks aan de Effectieve Leiding;
 - o De DPO is verantwoordelijk voor de implementatie van dit Beleid en ziet toe op de naleving van dit Beleid en van alle hiermee verbonden regelgeving door de Medewerkers;
 - o De DPO verstrekt advies met betrekking tot de DPIA en ziet toe op de uitvoering hiervan;
 - o De DPO fungeert als het contactpunt voor de Gegevensbeschermingsautoriteit en werkt er mee samen.
 - Compliance:
 - o Compliance herziet dit Beleid op regelmatige basis en minstens jaarlijks, in overeenstemming met het bepaalde in hoofdstuk VII.
 - Interne audit:
 - o Interne audit is verantwoordelijk voor het controleren en bevestigen van de adequaatheid en doeltreffendheid van het algemene kader voor de bescherming van Persoonsgegevens.

VI. Implementatie

1. Algemene verplichtingen

De verplichtingen van Quaestor inzake Persoonsgegevens hangen af van de hoedanigheid waarin zij optreedt. Wanneer Quaestor als Verwerkingsverantwoordelijke optreedt, en dus de beslissingen neemt over welke Persoonsgegevens Verwerkt worden, op welke manier, voor welk doel..., zal zij meer en andere verantwoordelijkheden hebben dan wanneer ze als Verwerker optreedt.

Quaestor zal voornamelijk als Verwerkingsverantwoordelijke optreden, aangezien Quaestor de partij is die de Persoonsgegevens zal verzamelen van de personen die in een onderliggende AICB zullen beleggen of waaraan ze beleggingsdiensten verlenen. Ook voor het Verwerken van Persoonsgegevens van haar werknemers en van derden waarmee zij contracten sluit, zal ze als Verwerkingsverantwoordelijke worden gezien. Wanneer een onderliggende AICB bepaalde Persoonsgegevens verzamelt en nadien Quaestor vraagt om deze te Verwerken, binnen de grenzen bepaald door de AICB, zal Quaestor als Verwerker worden beschouwd.

2. Welke gegevens worden verwerkt

Persoonsgegevens die voor Quaestor vooral van belang zullen zijn, zijn onder andere:

- Identificatiegegevens: bv. voornaam, naam, adres, telefoonnummers, emailadressen, functie, kopieën van identiteitskaarten en paspoorten, rijbewijs, geboorteplaats en -datum;
- Professionele gegevens: bv. gegevens inzake de professionele functie van de persoon in de onderneming van een klant, details inzake aandeelhoudersregisters, vertegenwoordigings- en handtekenbevoegdheden, handtekeningen;
- Demografische gegevens: bv. leeftijd, geslacht, burgerlijke staat, nationaliteit;
- Gegevens van klanten: bv. contactpersoon van de klant, informatie inzake de uiteindelijke begunstigde van de klant;
- Gegevens van derden: bv. CV's, Persoonsgegevens noodzakelijk om een contract te sluiten;
- Gegevens van werknemers: bv. details inzake salaris, hospitalisatieverzekering, trainingen die gevolgd werden, aansprakelijkheidsverklaringen en performance assessments.

3. Basisbeginselen van gegevensbescherming²⁰

Bij het Verwerken van Persoonsgegevens zal Quaestor de basisbeginselen van gegevensbescherming in acht nemen, waaraan elke Verwerking dient te voldoen.

a. Rechtmatigheid, behoorlijkheid en transparantie

Quaestor zal Persoonsgegevens rechtmatig, behoorlijk en transparant tegenover de Betrokkene Verwerken.

- **Rechtmatig**: de Verwerking moet steunen op één van de volgende gerechtvaardigde Verwerkingsgronden:
 - o De Betrokkene heeft zijn toestemming gegeven;
 - o De Verwerking van Persoonsgegevens is noodzakelijk om een contract aan te gaan;
 - o De Verwerking van Persoonsgegevens is noodzakelijk om aan een wettelijke verplichting te voldoen;
 - o De Verwerking van Persoonsgegevens is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van Quaestor.
- **Behoorlijk**: Quaestor dient een eerlijke, loyale houding tegenover de Betrokkene te hanteren en de Betrokkene te informeren over risico's ter vermindering van onvoorziene ongunstige gevolgen.
- **Transparant**: Quaestor dient te verzekeren dat de informatie inzake de Verwerking van Persoonsgegevens gemakkelijk te begrijpen en gemakkelijk toegankelijk is. Deze dient dus in duidelijke

²⁰ In overeenstemming met art. 5 GDPR

en klare taal te worden gecommuniceerd. De informatie die moet worden meegedeeld betreft onder andere de identiteit van de Verwerkingsverantwoordelijke, de doeleinden van de Verwerking, de risico's en de rechten van Betrokkenen.

b. Doelbinding

Persoonsgegevens moeten worden verkregen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Gegevens die voor een bepaald doeleinde zijn Verwerkt, mogen niet worden gebruikt voor andere doeleinden en moeten stroken met wat de Betrokkene redelijkerwijze kan verwachten. Zo kunnen bijvoorbeeld gegevens die worden verzameld met het oog op het sluiten van een contract met een klant, nadien niet gebruikt worden om hen marketing e-mails te sturen zonder hun uitdrukkelijke toestemming hiertoe te hebben verkregen.

c. Minimale gegevensverwerking

Volgens het beginsel van minimale gegevensverwerking mogen enkel die Persoonsgegevens verwerkt worden die noodzakelijk zijn voor het doeleinde waarvoor ze worden Verwerkt. Enkel het minimum mag dus worden verwerkt. Daarnaast moeten ze ook toereikend en ter zake dienend zijn.

d. Juistheid

De Persoonsgegevens die worden verwerkt moeten juist en up-to-date zijn. Het is de taak van Quaestor om alle redelijke maatregelen te nemen om de gegevens juist en volledig te houden en ze eventueel te verwijderen of aan te passen wanneer ze niet juist meer zijn.

e. Opslagbeperking

Quaestor mag de Persoonsgegevens niet langer bewaren dan noodzakelijk voor de verwezenlijking van de Verwerkingsdoeleinden. Wanneer dit doel is verwezenlijkt, moeten de gegevens worden verwijderd of geanonimiseerd, waardoor de identificatie van de Betrokkene niet meer mogelijk is. Quaestor bepaalt hiervoor redelijke opslagtermijnen en eventueel een periodieke reviewtermijn. Hoe lang Quaestor de gegevens bewaart en hoe deze na het verstrijken van die termijn eventueel worden verwijderd, wordt uiteengezet in het Gegevensbewaringsbeleid.

f. Integriteit en vertrouwelijkheid

Quaestor moet voorzien in passende technische en organisatorische maatregelen die ervoor zorgen dat een afdoende veiligheidsniveau wordt gehanteerd bij het Verwerken van de Persoonsgegevens. Hieronder wordt verstaan dat men zich moet beschermen, niet alleen tegen onrechtmatige Verwerking van gegevens, maar ook tegen bijvoorbeeld het verlies of diefstal van deze gegevens. Quaestor moet er dus voor zorgen dat de toegang tot de Persoonsgegevens wordt beschermd en beperkt tot diegenen die ze nodig hebben.

g. Doorgeven van Persoonsgegevens

Quaestor verkoopt nooit Persoonsgegevens aan derden. Zij zal wel in bepaalde gevallen Persoonsgegevens uitwisselen met derde partijen. Wanneer gegevens worden doorgegeven aan derde partijen, controleert Quaestor of de bescherming van Persoonsgegevens wordt gegarandeerd. Zo zorgt zij ervoor dat alle maatregelen worden genomen om te verzekeren dat enkel personen waarvoor de toegang tot de Persoonsgegevens noodzakelijk is voor het uitoefenen van hun taak toegang hebben. Daarnaast voorziet Quaestor in de nodige samenwerkingsovereenkomsten voldoende bescherming.

Partijen waar Quaestor Persoonsgegevens aan kan doorgeven:

- Verbonden ondernemingen en AICB's beheerd door Quaestor

Voor sommige doeleinden wisselt Quaestor gegevens uit met verbonden ondernemingen of met AICB's die door haar worden beheerd. Wanneer Quaestor gegevens uitwisselt, worden alle maatregelen genomen om te verzekeren dat enkel die personen toegang nodig hebben tot de Persoonsgegevens als dat noodzakelijk is voor het uitoefenen van hun taak.

- Specifieke dienstverleners

Om operationele redenen doet Quaestor soms beroep op specifieke dienstverleners. Deze worden telkens zorgvuldig geselecteerd en Quaestor neemt voldoende maatregelen om een adequate samenwerkingsovereenkomst te voorzien die voldoende bescherming biedt wat betreft Persoonsgegevens. Dergelijke samenwerkingsovereenkomsten moeten steeds aan Compliance worden voorgelegd ter goedkeuring.

- Overheidsinstanties

In sommige gevallen is Quaestor verplicht om bepaalde Persoonsgegevens mee te delen aan overheidsinstanties zoals de FSMA of de CTIF-CFI. Dit is bijvoorbeeld in het kader van de antiwitwaswetgeving.

h. Verantwoordingsplicht

Quaestor dient de naleving met deze basisbeginselen te kunnen aantonen.

i. Bijzondere aandacht bij het Verwerken van de gegevens buiten de EU

Niet-EU landen beschikken vaak niet over een regelgevend kader dat evenveel bescherming inzake gegevensverwerking biedt als de GDPR. Wanneer Quaestor Persoonsgegevens Verwerkt buiten de EU, dient zij daarom uitermate voorzichtig te zijn. Eerst en vooral heeft de Europese Commissie een lijst met landen die een adequaat beschermingsniveau hebben. In deze landen mogen Persoonsgegevens worden Verwerkt²¹. Wanneer Quaestor Persoonsgegevens wenst te zenden naar landen buiten de EU die geen adequaat beschermingsniveau hebben, kunnen Persoonsgegevens enkel worden Verwerkt wanneer Quaestor en de Verwerker buiten de EU passende waarborgen hebben geconstrueerd of contractuele bepalingen in werking zijn die ervoor zorgen dat toch voldoende bescherming met

²¹ De geactualiseerde lijst van bestemmingen met een passend beschermingsniveau kan worden geraadpleegd op https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

betrekking tot de Verwerking van de Persoonsgegevens kan worden verzekerd. Gelet op de huidige en de geplande toekomstige activiteiten van Quaestor, zal een Verwerking van Persoonsgegevens buiten de EU hoogstwaarschijnlijk niet voorkomen.

4. Rechten van de Betrokkene

a. Uitoefening van de rechten

De Betrokkene heeft verschillende rechten wanneer zijn Persoonsgegevens worden Verwerkt door Quaestor. Deze worden in punten b tot en met j van dit Hoofdstuk verder toegelicht.

Wanneer de Betrokkene een van deze rechten wenst uit te oefenen, neemt hij/zij contact op met de DPO:

- Tom Decloedt;
- tom.decloedt@quaestor.be;
- +32 51 26 33 60.

Indien een andere Medewerker een verzoek ontvangt van een Betrokkene, zendt hij/zij het verzoek door aan de DPO.

De DPO registreert elk verzoek in een door hem op te stellen register, te weten het Register inzake Verzoeken voor de Uitoefening van Rechten van de Betrokkene. Het register bevat op zijn minst volgende informatie:

- Nummer van het verzoek;
- Datum van het verzoek;
- Naam van de Betrokkene;
- Over welk recht het verzoek gaat;
- Of er al dan niet gevolg aan wordt gegeven;
 - o Indien niet, waarom niet;
 - o Indien wel, hoe Quaestor gevolg geeft aan het verzoek;
- Wat de gevolgen zijn voor Quaestor;
- Welke maatregelen Quaestor eventueel neemt;
- Of er verdere opvolging nodig is of al heeft plaatsgevonden..

b. Recht op informatie en transparantie

De Betrokkene heeft het recht om bepaalde informatie te ontvangen omtrent de Verwerking van zijn/haar Persoonsgegevens. De inhoud van deze informatieplicht hangt af van de situatie of de Persoonsgegevens al dan niet van de Betrokkene zelf zijn verkregen.

Wanneer de Persoonsgegevens bij de Betrokkene worden verzameld, verstrekt Quaestor deze informatie bij verkrijging van de Persoonsgegevens.

Wanneer de Persoonsgegevens niet van de Betrokkene zijn verkregen, verstrekt Quaestor de informatie:

- Zo snel mogelijk na verkrijging van de Persoonsgegevens en uiterlijk binnen één maand na verkrijging ervan;
- Indien de Persoonsgegevens zullen worden gebruikt voor communicatie met de Betrokkene, uiterlijk op het moment van het eerste contact met de Betrokkene; of
- Indien verstrekking van de gegevens aan een andere ontvanger wordt overwogen, uiterlijk op het tijdstip waarop de Persoonsgegevens voor het eerst worden verstrekt.

Een overzicht hiervan is terug te vinden in de Bijlage A van dit Beleid.

c. Recht van inzage

De Betrokkene heeft het recht om te weten of Quaestor al dan niet Persoonsgegevens van hem Verwerkt en indien dit zo is, welke Persoonsgegevens Quaestor over hem heeft. Daarnaast heeft de Betrokkene ook het recht op inzage van bijkomende informatie, die wordt opgesteld in Bijlage B.

d. Recht op rectificatie

De Betrokkene kan onverwijld rectificatie van onjuiste Persoonsgegevens vragen die op hem/haar betrekking hebben of, rekening houdend met het doel van de Verwerking, de vervollediging van onvolledige Persoonsgegevens vragen, inclusief via het maken van een bijkomende verklaring.

e. Recht op verwijdering van de Persoonsgegevens (“recht op vergetelheid”)

De Betrokkene heeft het recht om zonder redelijke vertraging de verwijdering van zijn Persoonsgegevens te verkrijgen wanneer:

- De Persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor ze verzameld waren;
- Hij zijn toestemming intrekt en er geen andere rechtsgrond was om de gegevens te mogen Verwerken;
- Hij bezwaar indient tegen de Verwerking en er geen prevalerende dwingende gerechtvaardigde gronden zijn voor de Verwerking;
- Hij bezwaar indient tegen de Verwerking van Persoonsgegevens ten behoeve van direct marketing;
- Er onrechtmatige Verwerking is van Persoonsgegevens;
- Er een wettelijke verplichting bestaat op het wissen van de Persoonsgegevens;
- De Persoonsgegevens verzameld zijn in verband met een aanbod van diensten van de informatiemaatschappij;

o Dit is bijvoorbeeld het geval wanneer de website van Quaestor financiële informatie over bepaalde genoteerde bedrijven gratis aanbiedt en hiervoor een e-mailadres of andere Persoonsgegevens opvraagt.

Indien Quaestor de Persoonsgegevens gedeeld heeft met anderen (ontvangers), dienen zij deze ook op de hoogte te brengen en te verzoeken om deze gegevens te wissen, tenzij dit onmogelijk is of onredelijk veel inspanning vereist.

Het recht op verwijdering van Persoonsgegevens is echter niet absoluut. Quaestor kan dit weigeren indien de Verwerking nodig is voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie, voor het nakomen van een wettelijke verplichting of voor het vervullen van een taak van het algemeen belang.

f. Recht op beperking van de Verwerking

De Betrokkene kan een beperking van de Verwerking van zijn Persoonsgegevens verzoeken. De beperking kan worden verzocht in volgende gevallen:

- De juistheid van de gegevens wordt betwist;
- De Verwerking is onrechtmatig;
- De Betrokkene heeft bezwaar gemaakt tegen de Verwerking.

Wanneer de Verwerking beperkt is, mag Quaestor de gegevens enkel bewaren. Verdere Verwerking van de gegevens is enkel mogelijk met toestemming van de Betrokkene of in bepaalde uitzonderingsgevallen.

g. Recht op overdraagbaarheid

De Betrokkene heeft het recht om de Persoonsgegevens die zij heeft verstrekt, in een gestructureerd, gangbaar en machine-leesbaar formaat te ontvangen en deze over te dragen aan derde partijen. Dit recht bestaat enkel indien (1) de Verwerking op toestemming of een contract rust en (2) de Verwerking via geautomatiseerde procedés verloopt.

h. Recht van bezwaar

De Betrokkene heeft het recht om bezwaar uit te oefenen tegen de Verwerking van zijn Persoonsgegevens wanneer:

- De Verwerking gebaseerd is op de vervulling van een taak van algemeen belang;
- De Verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van Quaestor.

Quaestor staakt in dat geval de Verwerking, tenzij dwingende, gerechtvaardigde gronden zwaarder wegen dan de belangen, rechten of vrijheden van de Betrokkene of in het kader van het instellen, uitoefenen of onderbouwen van een rechtsvordering.

Indien de Persoonsgegevens ten behoeve van direct marketing²² worden Verwerkt, heeft de Betrokkene altijd het recht om bezwaar te maken, ook al is de Verwerking niet gebaseerd op een van twee bovenstaande rechtvaardigingsgronden. In dit geval zal Quaestor de Persoonsgegevens niet meer Verwerken voor deze doeleinden.

i. Recht om niet aan geautomatiseerde besluitvorming te worden onderworpen

Quaestor heeft speciale aandacht voor het Verwerken van Persoonsgegevens en het nemen van besluiten hierover op basis van geautomatiseerde besluitvorming. Geautomatiseerde besluitvorming is de manier van besluitvorming waarbij een beslissing wordt genomen, gebaseerd op technologie, en dit zonder menselijke tussenkomst.

Het nemen van besluiten uitsluitend op basis van geautomatiseerde besluitvorming is verboden wanneer dit besluit rechtsgevolgen heeft voor de Betrokkene of hem op een andere manier in aanmerkelijke mate treft. In dat geval heeft de Betrokkene recht op menselijke tussenkomst, verzamelen van persoonsgegevens van (potentiële) klanten, het bepalen van algemene of specifieke klantenprofielen, om vervolgens het aanbod te kunnen afstemmen op de behoeften van de klant en het toezenden van gepersonaliseerde communicatie aan hem, behoudens in bepaalde uitzonderingen. Zo is deze manier van besluitvorming wel toegelaten in het kader van het controleren en voorkomen van belastingfraude.

j. Recht op facilitering van de uitoefening van deze rechten

Quaestor is verplicht om de uitoefening van bovenstaande rechten te faciliteren door een gevolg te geven aan de verzoeken van de Betrokkene inzake deze rechten. Bij het Verwerken van Persoonsgegevens van Betrokkenen, is Quaestor verplicht om op verzoek van de Betrokkene onverwijld en ten laatste binnen één maand hem mee te delen hoe zijn gegevens worden Verwerkt. In sommige complexe gevallen wordt deze termijn verlengd met twee maanden. Quaestor is echter niet verplicht om onredelijke verzoeken in te willigen, maar dient dan onverwijld en binnen één maand mee te delen waarom het verzoek zonder gevolg is gebleven. Dergelijke onredelijke verzoeken zijn bijvoorbeeld repetitieve of manifest ongegronde verzoeken.

5. Maatregelen om de naleving van de GDPR-verplichtingen te garanderen

Quaestor zal haar naleving van de GDPR op volgende wijze verzekeren:

• De nodige contracten opstellen

Quaestor stelt de nodige contracten met derde partijen op om de hoedanigheid waarin de contractspartijen optreden vast te leggen en om te verzekeren dat de basisprincipes van gegevensbescherming bij de uitvoering van het contract worden gerespecteerd.

²² Direct marketing is een algemeen Verwerkingsdoel en omvat een aantal verschillende activiteiten, zoals het verzamelen van persoonsgegevens van (potentiële) klanten, het bepalen van algemene of specifieke klantenprofielen, om vervolgens het aanbod te kunnen afstemmen op de behoeften van de klant en het toezenden van gepersonaliseerde communicatie aan hen.

• **Register van de Verwerkingsactiviteiten opstellen**

Quaestor stelt een register op waarin wordt bijgehouden welke data Verwerkt worden, voor welke doeleinden de Verwerking plaatsvindt, alsook andere wettelijk bepaalde elementen. Quaestor houdt dit register ter beschikking van de GBA.

• **Passende technische en organisatorische maatregelen nemen**

Quaestor neemt passende technische en organisatorische maatregelen om de gegevensbeschermingsbeginselen op een doeltreffende manier uit te voeren en de nodige waarborgen in te bouwen ter naleving van de wetgeving en ter bescherming van de rechten van de Betrokkenen.

Om de veiligheid van de Persoonsgegevens te garanderen, dient elke Medewerker de richtlijnen informatieveiligheid na te leven (zie bijlage C).

Verder wordt het Informatiebeveiligingsbeleid zo opgesteld dat enkel Medewerkers die toegang nodig hebben tot de Persoonsgegevens toegang hebben tot het medium waar die Persoonsgegevens zijn opgeslagen. Daarnaast wordt er gebruik gemaakt van Pseudonimisering en encryptie van bestanden die Persoonsgegevens bevatten. Dit wordt verder uiteengezet in het Informatiebeveiligingsbeleid.

Daarnaast zal Compliance de technische en organisatorische maatregelen jaarlijks evalueren en indien nodig aanpassen om te allen tijde de veiligheid van Persoonsgegevens te garanderen.

• **Data Protection Impact Assessment (DPIA) opstellen indien nodig**

Wanneer de Verwerking van Persoonsgegevens waarschijnlijk een hoog risico oplevert, is Quaestor verplicht een DPIA uit te voeren. Dit is bijvoorbeeld nodig wanneer gewerkt wordt met Profilering of een grote hoeveelheid Gevoelige Gegevens wordt Verwerkt. Quaestor beroept zich hierbij op de tussenkomst van de DPO, die bepaalt of een DPIA al dan niet nodig is.

• **Verantwoordelijke personen en aanspreekpunten aanstellen inzake alles wat met gegevensbescherming te maken heeft**

- o Quaestor stelt een DPO aan, die de in Hoofdstuk V. uiteengezette verantwoordelijkheden heeft;
- o Er worden procedures en beleidslijnen opgesteld, die de toepassing van de wetgeving inzake gegevensbescherming verzekeren;
- o De DPO houdt Medewerkers op de hoogte en geeft trainingen inzake de wetgeving, procedures en beleidslijnen omtrent gegevensbescherming;
- o Er worden privacy verklaringen voorzien in de communicatie met Medewerkers, klanten en derden.

6. Verwerking van bepaalde categorieën van Persoonsgegevens

Bepaalde categorieën van Persoonsgegevens vergen extra bescherming omdat het hier gaat om gevoelige Persoonsgegevens (“Bijzondere categorieën van Persoonsgegevens”).

a. Gevoelige gegevens

Verwerking van deze Persoonsgegevens is in principe verboden, behoudens bepaalde uitzonderingen, waaronder:

- De Betrokkene heeft zijn uitdrukkelijke toestemming gegeven;
- Deze data is vereist om de wettelijke verplichtingen uit het arbeids- of sociale zekerheidsrecht na te leven;
- Deze data is vereist om juridisch advies te kunnen verkrijgen of op een andere manier zijn rechten te kunnen uitoefenen of verdedigen.

In principe zal Quaestor geen Gevoelige gegevens Verwerken. Indien dergelijke Verwerking toch noodzakelijk is, neemt de Medewerker contact op met Compliance en vraagt toestemming aan Compliance om deze gegevens te Verwerken. Compliance kijkt dan na of (i) Quaestor de Verwerking van die Gevoelige Gegevens nodig acht en (ii) indien ja, of er een rechtsgrond bestaat voor de Verwerking van die Persoonsgegevens. Indien toestemming nodig is van de Betrokkene om de Gevoelige Gegevens te Verwerken, vraagt de Verantwoordelijke voor de Klantenrelaties de toestemming van de Betrokkene.

b. Strafrechtelijke veroordelingen en feiten

Verwerking van Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten is verboden, behalve indien er een wettelijke basis is. Dit is bijvoorbeeld het geval in het kader van antiwitwaswetgeving. In principe zal Quaestor enkel Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten Verwerken in het kader van de Antiwitwaswet²³. Indien deze gegevens voor een andere reden worden Verwerkt, neemt de Medewerker contact op met Compliance en vraagt toestemming aan Compliance om deze gegevens te Verwerken. Compliance kijkt dan na of (i) Quaestor de Verwerking van die Persoonsgegevens nodig acht en (ii) indien ja, of er een rechtsgrond bestaat voor de Verwerking van die Persoonsgegevens. Indien toestemming nodig is van de Betrokkene om de Persoonsgegevens te Verwerken, vraagt de Verantwoordelijke voor de Klantenrelaties de toestemming van de Betrokkene.

c. Kinderen

Een laatste categorie die een speciale waakzaamheid vereist zijn Persoonsgegevens van Kinderen. Deze worden extra beschermd en daarnaast is toestemming van de ouder of voogd nodig vooraleer deze mogen worden Verwerkt. De informatie inzake Gegevensverwerking die tot een Kind gericht is, dient toegankelijk, duidelijk en eenvoudig te zijn. Indien dergelijke Verwerking zich voordoet, neemt de Medewerker contact op met Compliance en vraagt toestemming aan Compliance om deze gegevens te Verwerken. Compliance kijkt dan na of (i) Quaestor de Verwerking van die Persoonsgegevens nodig acht en (ii) indien ja, of er een rechtsgrond bestaat voor de Verwerking van die Persoonsgegevens. Indien toestemming nodig is van de Betrokkene om de Persoonsgegevens te Verwerken, vraagt de Verantwoordelijke voor de Klantenrelaties de toestemming van de Betrokkene.

²³ Wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten

7. Melding en registratie van inbreuken (datalekken)

a. Interne melding

Iedere Medewerker is verplicht de DPO onmiddellijk te verwittigen in volgende gevallen:

- Bij een inbreuk op dit Beleid; of
- Bij verlies, onrechtmatige toegang of overdracht van Persoonsgegevens. Elke melding gebeurt via e-mail of telefonisch aan de DPO:
- Tom Decloedt;
- tom.decloedt@quaestor.be;
- +32 51 26 33 60.

b. Melding aan de Betrokkene

De Verantwoordelijke voor de Klantenrelaties informeert de Betrokkene van de inbreuk zonder onredelijke vertraging wanneer blijkt dat, na analyse door de DPO, de inbreuk in verband met de Persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Een melding aan de Betrokkene is niet nodig wanneer:

- Passende technische en organisatorische maatregelen zijn getroffen die zijn toegepast op de Persoonsgegevens waarop de inbreuk betrekking heeft. Dit houdt in dat de Persoonsgegevens onbegrijpelijk zijn gemaakt voor onbevoegden, door deze te pseudonimiseren of te anonimiseren;
- Quaestor achteraf maatregelen genomen heeft om ervoor te zorgen dat voormeld risico zich niet meer zal voordoen; of
- De melding onevenredige inspanningen zou vergen, waarbij een openbare mededeling in de plaats komt. Dit kan door bijvoorbeeld een banner op de Website van Quaestor omtrent het datalek te plaatsen.

De melding bevat op zijn minst de volgende gegevens:

- Wat de aard van de inbreuk is;
- De naam en de contactgegevens van de DPO;
- De waarschijnlijke gevolgen van de inbreuk;
- De voorgestelde of genomen maatregelen om de inbreuk zo veel mogelijk te beperken.

De melding gebeurt rechtstreeks aan de Betrokkene per post of via email overeenkomstig de template in Bijlage D van dit Beleid.

c. Melding aan de GBA

De DPO stelt de GBA zo snel mogelijk en niet later dan 72 uur nadat hij er kennis van heeft genomen in kennis van de inbreuk in verband met Persoonsgegevens. De melding is niet nodig wanneer het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. De melding aan de GBA gebeurt via het elektronisch formulier, te raadplegen op de Website van de GBA (Melding van een gegevenslek (V2.0) (gegevensbeschermingsautoriteit.be)). Het formulier wordt verzonden naar de GBA via het eforms-webportaal (Formulier opladen (autoriteprotectiondonnees.be)).

d. Registratie van inbreuken

Compliance documenteert intern alle inbreuken in verband met Persoonsgegevens in het Register Datalekken.

Dit register bevat de volgende gegevens:

- De datum waarop het datalek plaatsvond;
- De datum en het tijdstip waarop Quaestor het datalek ontdekt heeft;
- De naam van de Medewerker die het datalek ontdekt heeft;
- Het type datalek (bv. een USB-stick verloren waar Persoonsgegevens op staan);
- Het type Persoonsgegevens dat gelekt is (bv. salarisgegevens);
- Een inschatting van het aantal personen waarvan de Persoonsgegevens zijn gelekt;
- Hoe het datalek heeft kunnen gebeuren (bv. de USB-stick werd door een Medewerker verloren op café);
- De (mogelijke) gevolgen van het datalek;
- Of er een melding aan de GBA is gebeurd;
 - o Indien ja, wanneer de melding gebeurd is, door wie, hoe, etc.
 - o Indien neen, waarom niet;
- Of de melding tijdig werd gedaan (binnen de 72 uur);
- Of er een melding aan de Betrokkenen is gebeurd;
 - o Indien ja, wanneer de melding gebeurd is, door wie, hoe, etc.;
 - o Indien neen, waarom niet;
- Welke maatregelen Quaestor heeft getroffen om toekomstige lekken te voorkomen.

VII. Administratie

De Compliance functie is verantwoordelijk voor de naleving van dit Beleid door elke persoon werkzaam binnen Quaestor.

De Compliance functie zal dit Beleid periodiek en minstens jaarlijks herzien. De Raad van Bestuur beoordeelt minstens eenmaal per jaar of het Persoonsgegevensbeleid aangepast is aan de activiteiten van de instelling.

De Compliance functie zal dit Beleid aanpassen wanneer nodig. Aanpassingen kunnen bijvoorbeeld noodzakelijk zijn door:

- Wijzigingen in de relevante wetgeving;
- Wijzigingen in de activiteiten of diensten van Quaestor;
- Organisatorische wijzigingen van Quaestor.

Bovenstaande opsomming is niet-exhaustief.

Wanneer een update van dit Beleid significante aanpassingen met zich meebrengt, zullen deze aanpassingen ter goedkeuring worden voorgelegd aan de Raad van Bestuur van Quaestor. De Compliance verantwoordelijke mag geringe aanpassingen maken in het Beleid, zoals aanpassingen die verbonden zijn aan een herbenoeming van bepaalde diensten van Quaestor.

Quaestor heeft dit document in het Nederlands opgemaakt. Indien er enig conflict ontstaat tussen de Nederlandstalige versie van dit Beleid en een vertaling hiervan, zal de Nederlandstalige versie prevaleren.

De Compliance functie bewaart de vorige versies van dit Beleid gedurende 5 jaar.

Dit Beleid treedt in werking op 11/09/2023.

Bijlage A. Informatie te verstrekken aan de Betrokkene

Quaestor verstrekt volgende informatie aan de Betrokkene wanneer de Persoonsgegevens bij de Betrokkene zelf worden verzameld:

- De identiteit en de contactgegevens van de Verwerkingsverantwoordelijke en, in voorkomend geval, van de vertegenwoordiger van de Verwerkingsverantwoordelijke;
- (in voorkomend geval) de contactgegevens van de DPO;
- De Verwerkingsdoeleinden waarvoor de Persoonsgegevens zijn bestemd, alsook de rechtsgrond voor de Verwerking;
- Indien de Verwerking steunt op gerechtvaardigde belangen van Quaestor, wat deze gerechtvaardigde belangen inhouden;
- (in voorkomend geval) de ontvangers of categorieën van ontvangers van de Persoonsgegevens;
- (in voorkomend geval) het voornemen van de Verwerkingsverantwoordelijke om de Persoonsgegevens door te geven aan een derde land of internationale organisatie; of er al dan niet een adequaatheidsbesluit van de Commissie bestaat; of in het geval van doorgiften in de zin van artikel 46, 47 of 49 GDPR, welke de passende of geschikte waarborgen zijn, hoe er een kopie van kan worden verkregen of waar deze kunnen worden geraadpleegd;
- De periode van opslag of, indien er geen vaste periode wordt vastgesteld, de criteria ter bepaling van die termijn;
- Het feit dat de Betrokkene recht op inzage, rectificatie, verwijdering, beperking, bezwaar en overdraagbaarheid heeft;
- Het feit dat de Betrokkene het recht heeft om zijn toestemming in te trekken;
- Het feit dat de Betrokkene het recht heeft om een klacht in te dienen bij de toezichthoudende autoriteit;
- Of de verstrekking van Persoonsgegevens een wettelijke of contractuele verplichting is, dan wel een noodzakelijke voorwaarde om een contract te sluiten, of de Betrokkene verplicht is de Persoonsgegevens te verstrekken en wat de gevolgen zijn indien hij dit niet doet;
- Het bestaan van geautomatiseerde besluitvorming en nuttige informatie over de onderliggende logica en het belang en de gevolgen van de Verwerking.

Het verstrekken van deze informatie is niet verplicht:

- Wanneer en voor zover de Betrokkene reeds over deze info beschikt.

Quaestor verstrekt volgende informatie aan de Betrokkene wanneer de Persoonsgegevens niet bij de Betrokkene zelf worden verzameld:

- De identiteit en de contactgegevens van de Verwerkingsverantwoordelijke en, in voorkomend geval, van de vertegenwoordiger van de Verwerkingsverantwoordelijke;

- (in voorkomend geval) de contactgegevens van de DPO;
- De Verwerkingsdoeleinden waarvoor de Persoonsgegevens zijn bestemd, alsook de rechtsgrond voor de Verwerking;
- De betrokken categorieën van Persoonsgegevens;
- (in voorkomend geval) de ontvangers of categorieën van ontvangers van de Persoonsgegevens;
- (in voorkomend geval) het voornemen van de Verwerkingsverantwoordelijke om de Persoonsgegevens door te geven aan een derde land of internationale organisatie; of er al dan niet een adequaatheidsbesluit van de Commissie bestaat; of in het geval van doorgiften in de zin van artikel 46, 47 of 49 GDPR, welke de passende of geschikte waarborgen zijn, hoe er een kopie van kan worden verkregen of waar deze kunnen worden geraadpleegd;
- De periode van opslag of, indien er geen vaste periode wordt vastgesteld, de criteria ter bepaling van die termijn;
- (in voorkomend geval) de gerechtvaardigde belangen waarop de Verwerking is gebaseerd;
- Het feit dat de Betrokkene recht op inzage, rectificatie, verwijdering, beperking, bezwaar en overdraagbaarheid heeft;
- Het feit dat de Betrokkene het recht heeft om zijn toestemming in te trekken;
- Het feit dat de Betrokkene het recht heeft om een klacht in te dienen bij een toezichthoudende autoriteit;
- De bron waar de Persoonsgegevens vandaan komen en, in voorkomend geval, of zij afkomstig zijn van openbare bronnen;
- Het bestaan van geautomatiseerde besluitvorming en nuttige informatie over de onderliggende logica en het belang en de gevolgen van de Verwerking voor de Betrokkene.

Het verstrekken van deze informatie is niet verplicht:

- Wanneer en voor zover de Betrokkene reeds over deze info beschikt;
- Wanneer het verstrekken van info onmogelijk blijkt of onevenredig veel inspanning zou vergen in de zin van art.14, lid 5b) van de GDPR;
- Wanneer het verkrijgen of verstrekken van de gegevens uitdrukkelijk is voorgeschreven bij Unie- of nationaal recht dat op de Verwerkingsverantwoordelijke van toepassing is en dat recht voorziet in passende maatregelen om de gerechtvaardigde belangen van de Betrokkene te beschermen; of
- Wanneer de Persoonsgegevens vertrouwelijk moeten blijven uit hoofde van een beroepsgeheim in het kader van Unierecht of nationaal recht, waaronder een statutaire geheimhoudingsplicht.

Bijlage B. Informatie waartoe de Betrokkene inzage kan krijgen

Wanneer de Betrokkene zijn recht op inzage uitoefent, kan hij/zij naast inzage van de Persoonsgegevens die door Quaestor worden verwerkt ook inzage krijgen tot volgende informatie:

- De Verwerkingsdoeleinden;
- De betrokken categorieën van Persoonsgegevens;
- De ontvangers of categorieën van ontvangers aan wie de Persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties;
- Indien mogelijk, de periode gedurende welke de Persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
- Dat de Betrokkene het recht heeft de Verwerkingsverantwoordelijke te verzoeken dat Persoonsgegevens worden gerectificeerd of gewist, of dat de Verwerking van hem betreffende Persoonsgegevens wordt beperkt, alsmede het recht tegen die Verwerking bezwaar te maken;
- Dat de Betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;
- Wanneer de Persoonsgegevens niet bij de Betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens;
- Het bestaan van geautomatiseerde besluitvorming, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die Verwerking voor de Betrokkene.

Bijlage C. Richtlijnen informatieveiligheid

De volgende richtlijnen dienen te worden nageleefd door alle Medewerkers die in de uitoefening van hun functie binnen Quaestor omgaan met Persoonsgegevens.

- Vernietig Persoonsgegevens op de juiste manier: versnipper papieren Persoonsgegevens of gooi ze in beveiligde containers. Het weggooien van Persoonsgegevens in een vuilnisbak is niet veilig.
- Bewaar papieren met Persoonsgegevens op een veilige plaats: laat geen papieren met Persoonsgegevens in het zicht liggen, zoals op je bureau. Bewaar de papieren met Persoonsgegevens achter slot en grendel en sluit ook de ramen en deuren van de bureaus aan het einde van je werkdag. Laat ook geen papieren met Persoonsgegevens liggen in gemeenschappelijke plaatsen, zoals aan de printer, het kopieermachine, in de koffieruimte of in vergaderzalen.
- Let op met het digitaal opslaan en doorgeven van Persoonsgegevens: sla Persoonsgegevens niet lokaal op je computer op, maar op de daartoe aangeduide beveiligde netwerklocatie. Email enkel Persoonsgegevens indien er geen alternatief is.
- Zorg voor een sterk wachtwoord voor al je toestellen: gebruik sterke wachtwoorden (zoals zinnen) en verander je wachtwoord regelmatig. Schrijf je wachtwoorden nergens op en geef ze nooit door aan andere personen. Dit geldt niet alleen voor je computer, maar ook voor je GSM, tablet etc. die mogelijk Persoonsgegevens kunnen bevatten.
- Ga veilig om met je computer: let op met mails van onbekende afzenders en phishingmails, klik geen linken en bijlages open wanneer je twijfelt over de betrouwbaarheid ervan en vergrendel je computer. Berg je computer veilig op en laat hem nooit onbeheerd achter.
- Wees waakzaam, gebruik je gezond verstand en behandel Persoonsgegevens alsof ze de jouwe zijn.

Bijlage D. Melding datalek aan de Betrokkene

Geachte Heer/ Mevrouw [naam klant],

Wij schrijven u om u op de hoogte te brengen van een datalek dat zich binnen onze organisatie heeft voorgedaan en dat gevolgen kan hebben voor de bescherming van uw Persoonsgegevens.

Bij het verlenen van diensten aan u, houdt Quaestor zich aan de regels inzake de bescherming van Persoonsgegevens zoals voorgeschreven door de algemene verordening gegevensbescherming (Verordening (EU) 2016/679, "GDPR"). Als zodanig heeft Quaestor een robuust kader opgezet dat erop is gericht uw Persoonsgegevens zo goed mogelijk te beschermen. Meer details over het kader dat Quaestor heeft opgezet, zijn te vinden in ons Persoonsgegevensbeleid, dat als bijlage bij deze brief is gevoegd en dat altijd op onze website kan worden geraadpleegd.

Ondanks het feit dat Quaestor solide maatregelen heeft genomen om uw Persoonsgegevens te beschermen, hebben wij vastgesteld dat er zich toch een datalek heeft voorgedaan met betrekking tot uw Persoonsgegevens.

[Informatie over de aard van de inbreuk]

[Waarschijnlijke gevolgen van de inbreuk]

[De voorgestelde of genomen maatregelen om de inbreuk zo veel mogelijk te beperken]

Wij zijn altijd beschikbaar om eventuele resterende vragen te beantwoorden. Voor meer informatie kan u altijd contact opnemen met onze Data Protection Officer:

[Naam DPO]

[Contactgegevens DPO]

Met vriendelijke groeten,

[Handtekening]

[Naam verantwoordelijke voor de klantenrelaties]