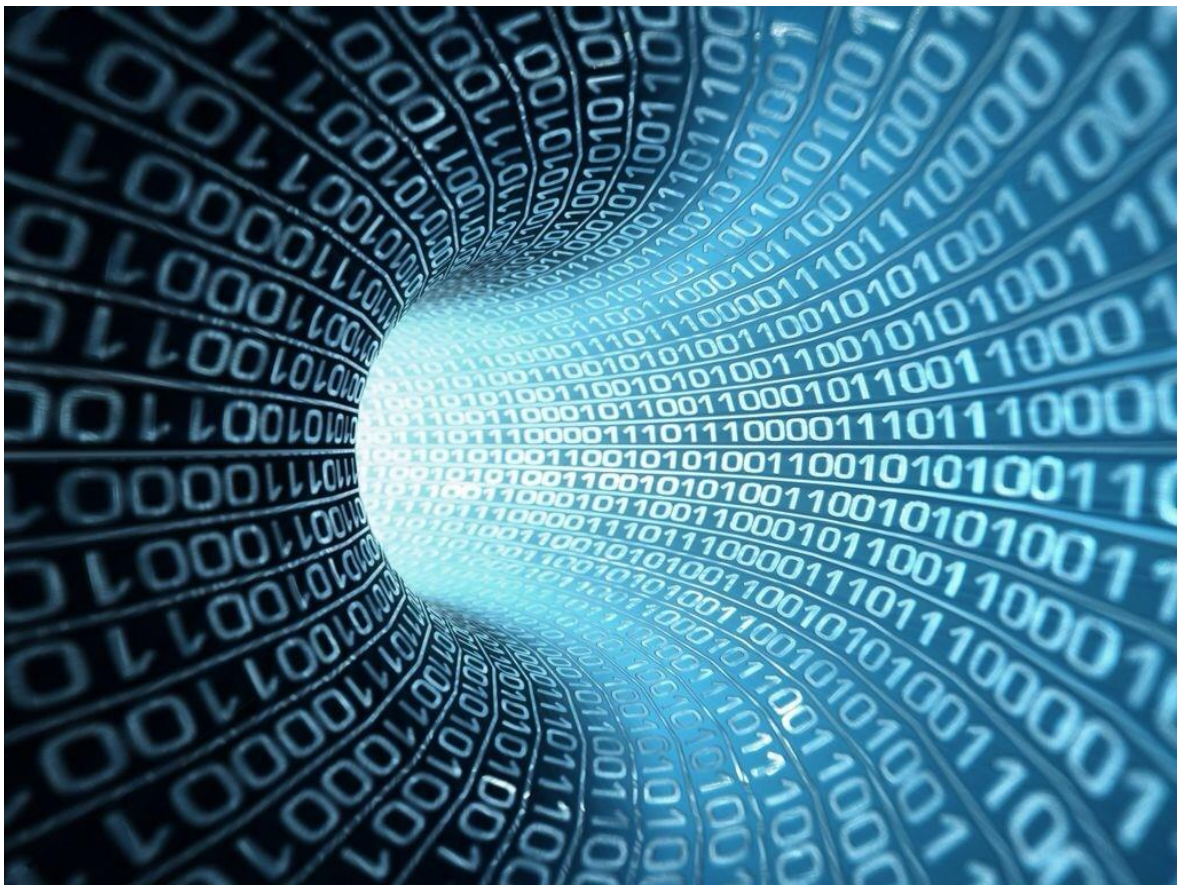
VASTGOED MANAGEMENT NEDERLAND

STAPPENPLAN

Wet bescherming persoonsgegevens (Wbp) / meldplicht datalekken

Versie 1.1 / 21 juli 2016



Disclaimer
Dit stappenplan met bijlagen is geen juridisch document of advies en beoogt niet volledig te zijn, maar geeft slechts een indicatie van bepaalde Wbp verplichtingen. Hetzelfde geldt ook voor het schema (pagina 5) dat een overzicht geeft van bepaalde Wbp verplichtingen, maar dus niet is bedoeld als juridisch advies en ook niet beoogt volledig te zijn. Voor u relevante bijlagen, links en handreikingen bundelt VGM NL voor u op haar website onder 'lopende dossiers'. VGM NL is niet aansprakelijk voor enige schade op welke wijze dan ook voortvloeiende uit (het gebruik van) verstrekte informatie.

Inhoud

Bijlagen

Dit Stappenplan is uitgegeven op 14 juni 2016 en gewijzigd op:

- *21 juli 2016; i.v.m. de toevoeging van de Bewerkersovereenkomst (met groepsvennootschap optie) ENG*

Inleiding

Sinds 1 januari 2016 geldt de nieuwe Wet datalekken die valt onder de Wet bescherming persoonsgegevens (Wbp) waarbij bepaalde datalekken moeten worden gemeld. Een datalek is een inbreuk op de bij wet vereiste beveiliging van persoonsgegevens waarbij kort gezegd (digitale of fysieke) persoonsgegevens verloren zijn gegaan of onrechtmatig zijn verwerkt. Hiervan kan bijvoorbeeld sprake zijn bij een zoekgeraakte USB-stick, een gestolen laptop of een inbraak door een hacker.

De Autoriteit Persoonsgegevens kan vanaf 1 januari 2016 organisaties een boete opleggen als zij de Wet bescherming persoonsgegevens overtreden. De maximale boete is € 820.000 of zelfs 10% van de jaaromzet voor een overtreding. Er zijn beleidsregels van de Autoriteit Persoonsgegevens met richtlijnen inzake onder andere de hoogte van de boete, klik hier >>

Aedes publiceerde in mei 2016 de 'handreiking gegevens bescherming'. Deze handreiking gaat dieper in op de wet en is geschreven voor de corporaties. Klik hier >>

Aanleiding Stappenplan

Deze ontwikkelingen zijn voor VGM NL aanleiding voor het opstellen van dit Stappenplan Wbp / datalekken. Het doel van dit Stappenplan is u bewust te maken van de risico's die u loopt als vastgoed- en/of VvE manager bij het hebben en gebruiken van persoonsgegevens. De stappen in deze checklist helpen u inzicht te krijgen in de huidige situatie van uw organisatie ten aanzien van de persoonsgegevens en naleving van de Wbp. De stappen in het stappenplan zijn niet volgtijdelijk bedoeld, maar zullen allen moeten worden gezet!

Wat zijn persoonsgegevens? En wat is verwerken?

Een vastgoed- en/of VvE manager werkt met persoonsgegevens, namelijk van (potentiële) huurders, contactpersonen van bedrijven, werknemers, eenmanszaken en VOF's (want de informatie van de eenmanszaak / VOF kan iets zeggen over de eigenaar). Daarom adviseren wij u onderstaande checklist te doorlopen en, waar nodig, actie te ondernemen.

Definitie persoonsgegevens:
Persoonsgegevens zijn gegevens betreffende geïdentificeerde of identificeerbare natuurlijke personen zoals hierboven genoemd.

Bij persoonsgegevens kunt u denken aan bijvoorbeeld: NAW-gegevens, leeftijd, geslacht, foto, telefoonnummer, email adres, gezondheid, burgerlijke staat, creditcard gegevens, IP adres en het burgerservicenummer (bsn).

Centraal staat verder het begrip verwerking van persoonsgegevens. Dit is elke handeling met betrekking tot persoonsgegevens zoals het verzamelen, gebruiken, opslaan, verstrekken, inzien, verwijderen en vernietigen van persoonsgegevens. Voor elke verwerking van persoonsgegevens moet worden voldaan aan de eisen van de Wbp.

Melding datalekken

Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) onverwijld (binnen 72 uur na ontdekking) een melding moeten doen bij de Autoriteit Persoonsgegevens:

1. als het datalek ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens; of
2. als de inbreuk leidt tot een aanzienlijke kans op ernstige nadelige gevolgen.

Zo is over het algemeen een melding noodzakelijk als het bijvoorbeeld gaat om:

- *Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp*
  zoals ras (denk ook aan foto / nationaliteit) en gezondheid;
- *Gegevens over de financiële of economische situatie van de betrokkene;*
  bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens;
- *(Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;*
  bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen;
- *Gebruikersnamen, wachtwoorden en andere inloggegevens;*
  De mogelijke gevolgen voor betrokkenen kunnen groter zijn dan in eerste instantie gedacht. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen;
- *Gegevens die kunnen worden misbruikt voor (identiteits)fraude;*
  onder meer biometrische gegevens, kopieën van identiteitsbewijzen en om het bsn.

De betrokkene moet onverwijld worden geïnformeerd als de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor zijn/haar persoonlijke levenssfeer. Het datalek hoeft echter niet te worden gemeld aan de betrokkene als:

1. passende technische beschermingsmaatregelen zijn genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens (bijvoorbeeld door encryptie); of
2. dit noodzakelijk is met het oog op bepaalde in de wet genoemde belangen, zoals bijvoorbeeld de bescherming van de betrokkene of de voorkoming van strafbare feiten.

Meer informatie is te vinden in de Beleidsregels meldplicht datalekken van de Autoriteit Persoonsgegevens, klik hier >>.
De melding kan worden gedaan door middel van een webformulier op de website van de Autoriteit Persoonsgegevens.

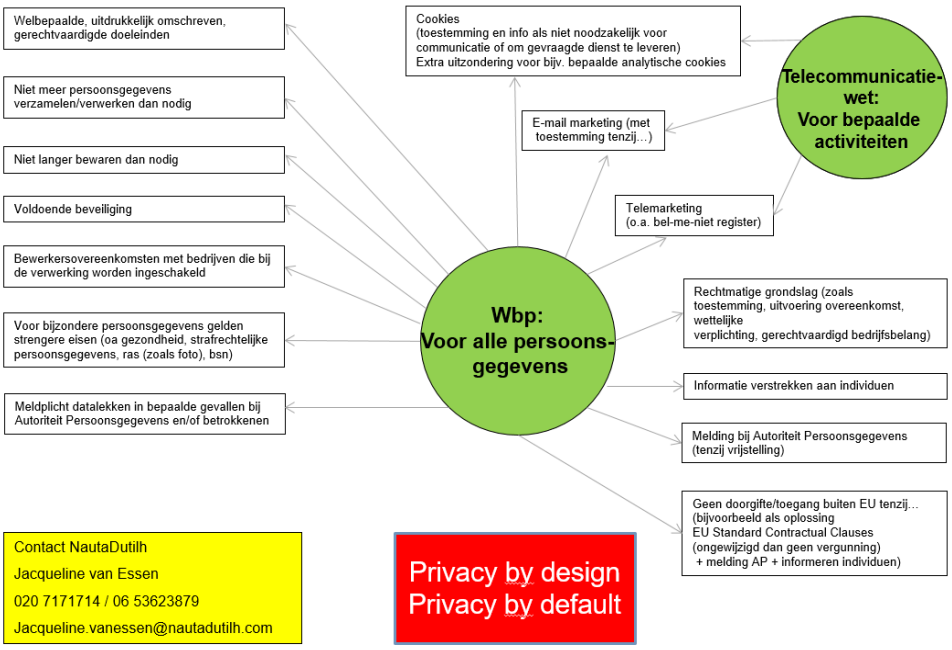
De verantwoordelijke binnen uw organisatie (meldingsplichtige) moet een overzicht bijhouden van de datalekken die onder de meldplicht vallen en heeft de meldingsplicht, niet de bewerker.

ADVIES

leg contractueel vast dat de bewerker verplicht is een datalek te melden aan de verantwoordelijke, zodat de verantwoordelijke hiervan op de hoogte is en tijdig de Autoriteit kan informeren waar nodig óf maak afspraken (en leg deze vast) dat de bewerker meldt namens de verantwoordelijke

STAPPENPLAN

Verplichtingen Wet bescherming persoonsgegevens (“Wbp”) en Telecommunicatiewet



Stap 1: Verzamel en verwerk niet meer persoonsgegevens dan nodig

Let op! Er zijn strenge regels ten aanzien van kopie paspoort / of ander identiteitsbewijs en/of het bsn. U mag in principe geen kopie paspoort / ander identiteitsbewijs maken en/of het bsn niet zomaar noteren / bewaren, tenzij er een wettelijke uitzondering is.
Lees hier meer over het ‘kopietje paspoort klik hier >>
Of op de website van de Autoriteit Persoonsgegevens klik hier >>
Meer informatie klik hier >>

De vastgoed- en VvE managers mogen dus geen kopie paspoort / ander identiteitsbewijs maken en het bsn mag niet worden genoteerd / bewaard.
De makelaar en bemiddelaar vallen onder de Wwft voor zover hun werkzaamheden zien op de aan- en verkoop van onroerende zaken. Op grond van de Wwft zijn zij verplicht om hun cliënt te identificeren en mag een kopie van het identiteitsbewijs (bijvoorbeeld een paspoort) worden gemaakt. Op grond van de Wwft moeten de identificatiegegevens (al dan niet opgeslagen door middel van een kopie van een identiteitsbewijs) van de cliënt worden bewaard gedurende vijf jaar na het tijdstip waarop de zakelijke relatie is beëindigd of de betreffende transactie is uitgevoerd. Wanneer de makelaar en bemiddelaar optreden in het kader van de totstandkoming van een huurovereenkomst, dan gelden de verplichtingen op grond van de Wwft niet, en mag dus ook geen kopie van een identiteitsbewijs worden gevraagd.

TIP
gebruik (indien het nodig is het ID bewijs te kopiëren) een ‘ID Cover’ of de app ‘KopieID’

De taxateur valt ook onder de Wwft, maar is niet verplicht de cliënt te identificeren. De taxateur mag derhalve geen kopie van een identiteitsbewijs maken.

In verband met het toekennen van huurtoeslag moet de verhuurder gegevens inzake het huurcontract, waaronder in elk geval begrepen de huurprijs van de woning alsmede een bsn

kunnen verstrekken aan de belastingdienst (op grond van artikel 38 Awir, jo artikel 1a lid 1 sub a en artikel 1b lid 2 Uitvoeringsbesluit Awir). Hiervoor mag de verhuurder het bsn vragen. Dit betekent niet dat ook kopie van een paspoort mag worden gemaakt.

Voorbeeld ID Cover: Klik hier >> of klik hier >>.

Stap 2: Maak een inventarisatie

Inventariseer binnen uw organisatie welke persoonsgegevens u verzamelt en bijbehorende informatie zoals:

- Welke persoonsgegevens verzamelt uw organisatie en welke worden vastgelegd?
- Met welke doelen?
- Hoe lang?
- Fysiek en/of digitaal?
- Aan wie worden de persoonsgegevens verstrekt? En met welk doelen?
- In welke systemen?
- Wie heeft er toegang tot deze systemen?

Bijlage 1: VGM NL Voorbeeld Inventarisatie

Stap 3: Bewaar persoonsgegevens niet langer dan nodig

Op grond van artikel 10 van de Wbp mogen persoonsgegevens niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren, dan *noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt*. Artikel 10 Wbp bevat geen concrete termijn hoe lang persoonsgegevens mogen worden bewaard. Richtlijnen voor wat geldt als een redelijke bewaartermijn zijn onder meer te vinden in het Vrijstellingsbesluit Wbp.

Een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, die voor de verwezenlijking van doeleinden of van verscheidene samenhangende doeleinden bestemd is, moet op grond van artikel 27 van de Wbp worden gemeld bij de Autoriteit Persoonsgegevens. Artikel 27 van de Wbp is niet van toepassing op verwerkingen van persoonsgegevens die zijn opgenomen in het Vrijstellingsbesluit Wbp ("Vrijstellingsbesluit").

Artikel 27 van de Wbp is op grond van artikel 14 van het Vrijstellingsbesluit niet van toepassing op de verwerking van gegevens met het oog op de huur of verhuur van roerende of onroerende zaken, waaronder tevens wordt begrepen het aanvragen en verstrekken van huurtoeslag. In de toelichting op het Vrijstellingsbesluit wordt vermeld dat deze vrijstelling ziet op de situatie dat de verantwoordelijke zelf optreedt als partij bij de rechtsverhouding in het kader waarvan de verwerking geschiedt (dit lijkt dus te zien op de eigenaar in plaats van een vastgoed- en/of VvE manager). Een andere mogelijkheid voor een vrijstelling tot melding zou artikel 13 'afnemers en leveranciers' kunnen zijn waar het gaat om verwerkingen van persoonsgegevens van afnemers of leveranciers of personen die in een soortgelijke relatie staan.

In het Vrijstellingsbesluit wordt per categorie vrijgestelde verwerking een eis gesteld aan de bewaartermijn. Deze bewaartermijn kan worden opgevat als een richtlijn voor wat als redelijke bewaartermijn geldt. In artikel 14 lid 5 van het Vrijstellingsbesluit is bepaald dat de

persoonsgegevens moeten worden verwijderd uiterlijk 2 jaar nadat de huur is geëindigd, met dien verstande dat de gegevens met betrekking tot de aanvraag en verstrekking van huurtoeslag worden verwijderd uiterlijk 5 jaar nadat de huurtoeslag is geëindigd, tenzij de persoonsgegevens noodzakelijk zijn ter voldoening aan een wettelijke bewaarplicht. In artikel 13 lid 5 van het Vrijstellingsbesluit wordt gerefereerd aan twee jaar nadat de transactie is afgehandeld, tenzij de persoonsgegevens noodzakelijk zijn ter voldoening aan een wettelijke bewaarplicht.

Voor de administratie van de vastgoed- en VvE managers geldt de algemene bewaartermijn van 7 jaar zoals deze is opgenomen in boek 2 van het burgerlijk wetboek voor rechtspersonen. Dit geldt ook voor de fiscale termijn van 7 jaar. Het huurdossier mag op grond van deze termijnen alleen worden bewaard wanneer het relevant is voor de eigen administratie.
Voor de vastgoedeigenaar geldt daarnaast een fiscale bewaartermijn van 10 jaar (9 jaar, volgend op het jaar waarin de ondernemer het is gaan gebruiken) in verband met herzieningstermijnen. Het is van belang dat de belastingdienst aan de hand van administratie en andere gegevens nog 10 jaar terug kan om vast te stellen of aftrek van voorbelasting op de juiste wijze heeft plaatsgevonden.

Bijlage 2: Overzicht relevante wettelijke bewaartermijnen huurdossier

Artikel 10 Wbp biedt in beginsel een ruimere grondslag om persoonsgegevens te bewaren dan opgenomen in het Vrijstellingsbesluit. Partijen kunnen belang hebben bij het bewaren van (stukken in) een dossier, zonder dat daar een duidelijke wettelijke grondslag onder ligt. Bijvoorbeeld omdat zij over bewijsstukken willen beschikken zolang een verjaringstermijn niet is verstreken. In de wet zijn verschillende verjaringstermijnen opgenomen. De meeste termijnen zijn vijf jaar na het opeisbaar worden van de vordering. De verjaringstermijn is geen wettelijke bewaartermijn, maar kan als (één van de) redenen worden gebruikt waarom een huurdossier langer wordt bewaard dan de hiervoor genoemde termijn van 2 jaar waar het Vrijstellingsbesluit vanuit gaat.
Dit kan dus leiden tot het moeten doen van een melding bij de Autoriteit Persoonsgegevens.

Het is van belang dat - als er geen duidelijke wettelijk grondslag is - kan worden onderbouwd waarom het noodzakelijk is om te beschikken over de gegevens.

Meer informatie over de meldingsplicht en een mogelijke vrijstelling vindt u hier: https://autoriteitpersoonsgegevens.nl/nl/melden/melden-verwerking-persoonsgegevens. Overleg met uw juridisch adviseur over de noodzaak tot het doen van een melding.

Stap 4: Zorg voor voldoende beveiliging

Binnen uw organisatie dient u voor voldoende beveiliging te zorgen t.b.v. de veiligheid van de persoonsgegevens. U dient zowel technische als organisatorische beveiligingsmaatregelen te treffen.
Hierbij hoort het nadenken over gegevensstromen, het vormen van een visie én het uitrollen van deze visie binnen uw organisatie om ‘awareness’ (bewustwording) te creëren.
De Autoriteit Persoonsgegevens heeft richtlijnen opgesteld ten behoeve van de beveiliging. Klik hier >>
Zorg onder meer voor geheimhoudingsverklaringen met alle medewerkers en help hen zich bewust te worden van het belang van beveiliging en de gevaren.

Bijlage 3: VGM NL Voorbeelden Beveiliging en Awareness

Stap 5: Zorg voor goede bewerkersovereenkomsten met leveranciers

Uw organisatie wordt als vastgoed- en/of VvE manager in het kader van de wet datalekken waarschijnlijk als 'verantwoordelijke' aangemerkt t.a.v. uw verwerking van persoonsgegevens in het kader van bijv. verhuur. Een 'verantwoordelijke' dient zelf (de organisatie) melding te doen bij de Autoriteit Persoonsgegevens én voor zover u externe leveranciers gebruikt die in uw opdracht persoonsgegevens verwerken (zogenaamde bewerkers) moeten zij u ook informeren over datalekken. Dit moet dus contractueel worden overeengekomen.

Bewerkersovereenkomsten moeten bepaalde wettelijke bepalingen bevatten en ook heeft de Autoriteit Persoonsgegevens richtlijnen opgesteld inzake bewerkersovereenkomsten. Zie bijvoorbeeld: Klik hier >>

Voorbeelden van bewerkers zijn:

- Salarisadministratiekantoor;
- IT leveranciers die systemen hosten waarop persoonsgegevens staan en/of hiervan onderhoud & support verzorgen;
- Property Management automatisering zoals SAP / Rems / Cubic Eyes / Realworks / Yardi, etc.

Bijlage 4: Bewerkersovereenkomst Vastgoed- en VvE Managers

TIP

overweeg in huurovereenkomsten een privacy melding (notice) toe te (laten) voegen

Stap 6: Wees transparant

Zorg ervoor dat de personen wiens persoonsgegevens uw organisatie verwerkt weten wie uw organisatie is en voor welke doeleinden uw organisatie hun persoonsgegevens verwerkt. Nadere informatie dient te worden verstrekt voor zover dat gelet op de aard van de gegevens of de omstandigheden nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen. Denkt u bijvoorbeeld aan het vermelden van (categorieën van) ontvangers zoals een eigenaar, informatie over het recht te verzoeken om inzage in persoonsgegevens en/of deze te verbeteren, aan te vullen, te verwijderen of af te schermen, informatie als persoonsgegevens worden doorgegeven naar, of toegankelijk zijn in, een land buiten de EU dat niet voldoende privacybescherming biedt. Deze informatie kan worden opgenomen in een privacy policy en kunt u ook op de website vermelden (met daarin ook informatie inzake cookies indien die worden geplaatst; zie hieronder). Een Privacy online generator tool vindt u hier >>.

Mocht u op uw website gebruik maken van cookies of andere automatische gegevensverzamelingsprocedures zoals web beacons of device fingerprinting dan gelden nog aanvullende regels als opgenomen in de Telecommunicatiewet.

Meer informatie treft u bijvoorbeeld hier >> en bij de Autoriteit Persoonsgegevens, klik hier >>.

Stap 7: Let op dat de persoonsgegevens niet buiten de EU gaan

Indien persoonsgegevens worden verstrekt aan ontvangers in landen buiten de EU of daar toegankelijk zijn, dient u te voldoen aan aanvullende regels / eisen. Bijvoorbeeld als u een opdrachtgever heeft die buiten de EU is. Lees hierover bijvoorbeeld meer bij de Autoriteit Persoonsgegevens: Klik hier >>

In veel gevallen zal uw organisatie een EU standaard model contract moeten sluiten met de ontvanger buiten de EU. Klik hier voor de link >> (u vindt hier 3 varianten).
Let op: deze documenten mogen niet aangepast te worden, want dan moet u ook een vergunning aanvragen!

Voorbeelden waar dit een rol kan spelen:

- Office 365 of andere gegevens verwerking in pakketten van opdrachtgevers die zich buiten de EU bevinden.
- Opdrachtgever buiten de EU die huurdersgegevens bij u opvraagt.

Stap 8: Zorg voor een beveiligingsincidentenprotocol

In de inleiding van dit stappenplan leest u meer over de melding van datalekken bij de Autoriteit Persoonsgegevens en/of betrokkenen.
Binnen uw organisatie zou er een protocol moeten zijn waarin informatie is opgenomen zoals:

- Wie is de contactpersoon binnen uw organisatie waar mensen datalekken kunnen melden?
- Wie maken er verder deel uit van het ‘datalek team’? Denk aan IT, communicatie, compliance, jurist, bestuur. Denk tevens aan externe IT leveranciers die kunnen helpen bij een mogelijke hack en/of andere externe adviseurs.
- Wie meldt datalekken waar nodig bij de Autoriteit Persoonsgegevens, bedrijven en/of betrokkenen? Wie doet waar relevant aangifte bij de politie etc.?

Bijlage 5: Voorbeeld Protocol Meldplicht Datalekken

Stap 9: Voorbereidingen voor de Privacy verordening

Vanaf 25 mei 2018 moet uw organisatie voldoen aan nieuwe regels. De Wbp vervalt dan en daarvoor in de plaats moet de EU Privacy Verordening worden nageleefd. Deze bevat deels dezelfde regels, maar ook nieuwe / uitgebreidere verplichtingen.
Voor de presentatie van NautaDutilh over de Wbp en Verordening klik hier >>.

TIP

vraag in alle gevallen juridisch advies!

Bijlage 1. VGM NL Voorbeeld Inventarisatie

Gegevensverwerking	Wat is het doel van de gegevensverwerking?	Van welke (categorieën) personen worden gegevens verwerkt?	Welke gegevens worden verwerkt?	Wie ontvangen gegevens uit de verwerking?	Doel delen gegevens met derden?	Welke automatiserings systemen?	Wie heeft toegang tot locatie van de gegevens?	Hoe lang worden gegevens bewaard?	Worden persoonsgegevens doorgegeven naar landen buiten de Europese Unie?	Digitaal/Papier
Verhuuradministratie										
Contractadminstratie										
Eigenaren Administratie										
Technische Administratie										
Debiteuren Administratie										
Assurantie Administratie										
Bedrijfshuisvesting										
Taxaties										
WE-Administratie										
Personeelsadministratie										

Het Exceloverzicht is te downloaden via onze website, achter de inlog, uitsluitend voor VGM NL leden.

Bijlage 2. Overzicht relevante wettelijke bewaartermijnen huurdossier

Wet	Omschrijving	Termijn	Wie
Artikel 2:10 Burgerlijk Wetboek	Verplichting tot het voeren van een administratie en bewaren van daartoe behorende boeken, bescheiden en andere gegevensdragers, zodat te allen tijde de rechten en verplichtingen van de rechtspersoon kunnen worden gekend.	7 jaar	Eigenaar, beheerder, makelaar en taxateur, voor zover huurdossier relevant is voor eigen administratie.
Artikel 52 algemene wet inzake rijksbelastingen	Gegevens over de vermogenstoestand van een bedrijf of een zelfstandig beroep, waaronder: boeken, bescheiden en andere gegevensdragers die van belang zijn voor de heffing van belasting.	7 jaar	Eigenaar, beheerder, makelaar en taxateur, voor zover huur-dossier relevant is voor eigen administratie.
Artikel 34a, wet op de omzetbelasting 1968	Gegevens betreffende de onroerende zaken en rechten waaraan deze zijn onderworpen, waaronder: boeken, bescheiden en andere gegevensdragers of de inhoud daarvan.	9 jaar, volgend op jaar waarin ondernemer het is gaan gebruiken. [vaak aangeduid als 10 jaar]	Eigenaar, beheerder / makelaar indien deze bewaart namens de eigenaar. Gaat met name om de huurovereenkomst.
Artikel 33, wet ter voorkoming van witwassen en financieren van terrorisme (Wwft)	Alle gegevens die in het kader van cliëntonderzoek (customer due diligence) zijn verkregen.	5 jaar	Makelaar en bemiddelaar in het kader van aan- en verkoop van onroerend goed. Taxateur als daartoe aanleiding bestaat. [niet voor huurdossiers]
Artikel 34 Wwft	Meldingen over ongebruikelijke transacties.	5 jaar	Makelaar, bemiddelaar en taxateur [niet voor huurdossier]

Bijlage 3: Voorbeelden Beveiliging en awareness (bewustwording)

Zorg voor trainingen, draag de visie op beveiliging en protocollen uit en herhaal de boodschap regelmatig. Hieronder sommen wij een aantal voorbeelden op, waar u aan kunt denken inzake een goede beveiliging.

Digitaal:

- ✓ Installeer geen software op uw kantoor PC zonder toestemming van de IT afdeling.
- ✓ Open geen verdachte E-mails / bijlagen gestuurd door mensen / bedrijven die u niet kent of vertrouwt.
- ✓ Klik niet op E-mail links (en in ieder geval niet als gevraagd wordt persoonlijke informatie op een website in te vullen). Twijfelt u over de rechtmatigheid van een email, bel uw bank, service provider, het bedrijf of de IT afdeling. Bel dan niet het nummer in de email.
- ✓ Als iemand van een externe IT afdeling, uw bank, service provider, Microsoft, Apple of een Antivirus software provider u belt en u vraagt websites te openen of software te installeren, verbreekt u dan alstublieft de verbinding en bel met de IT afdeling.
- ✓ Gebruik uw kantoor PC en telefoon (zoveel mogelijk) alleen voor bedrijfsdoeleinden.
- ✓ Gebruik sterke en unieke wachtwoorden en houd deze veilig.
- ✓ Houd uw software up-to-date na toestemming van de IT afdeling [bijv. als mensen een iphone e.d. hebben van de zaak, SW updates van de kantoor PC gaan centraal].
- ✓ Ga niet akkoord met vriendschaps/connectieverzoeken ontvangen per email (bijv. emails van LinkedIn, Facebook etc.). Ga eerst naar de websites van Facebook of LinkedIn via internet explorer en accepteer vervolgens op die website zelf dergelijke verzoeken.
- ✓ Gebruik geen zakelijke email adressen op persoonlijke websites of social media.
- ✓ Stop nooit een USB-stick die u ergens heeft gevonden of van iemand heeft gekregen die u niet kent of niet vertrouwt in uw PC.
- ✓ Rapporteer beveiligingsincidenten direct bij de IT afdeling (bijv. verlies van data, onrechtmatige verwerking / toegang, of kans daarop).
- ✓ Stuur geen zakelijke e-mails/documenten naar uw privé email adres (zoals hotmail / gmail).
- ✓ Open geen bestanden of documenten met .exe, .msi, .js or .vbs extensie zonder toestemming van de IT afdeling.
- ✓ Haal altijd laptop uit de auto.
- ✓ Bepaal hoe u wilt omgaan met Social Media binnen uw organisatie (vermenging privé en zakelijk / wat meld en plaats je hier en kijk uit met klant info + kritisch eigen profiel).
- ✓ Let op Privacy instellingen en verificatie en acceptatie van connectie verzoeken.
- ✓ Gebruik alleen ge-encrypte USB Sticks, laptops, tablets, etc.

Fysiek:

- ✓ Clean Desk policy.
- ✓ Gebruik de papierversnipperaar bij het weggooien van fysieke persoonsgegevens.
- ✓ Doe deuren en kasten op slot.
- ✓ Leg uit wat een datalek is.
- ✓ Creëer bewustzijn door herhaling, confrontatie en herkenning.
- ✓ Denk eraan dat persoonsgegevens niet zomaar gedeeld mogen worden met leveranciers en derden. Er moet worden voldaan aan de Wbp.
- ✓ Let op met onbekende bezoekers in het gebouw dat zij worden begeleid door een medewerker.
- ✓ Overweeg strenger aannamebeleid (screening, VOG).
- ✓ Classificatie en autorisatie van documenten.
- ✓ Overweeg toegangsbeleid.
- ✓ Wees alert en meld verdachte zaken.
- ✓ Durf te vragen.

Bijlage 4.a.: Bewerkersovereenkomst VGM standaard

DIT CONCEPT BEVAT STANDAARDBEPALINGEN EN IS TOT STAND GEKOMEN IN OVERLEG MET **NAUTADUTILH N.V.** OVERLEG WAAR NODIG MET UW JURIDISCH ADVISEUR OOK OP BASIS VAN DE SPECIFIEKE OMSTANDIGHEDEN EN ONDERHANDELINGEN.

DIT CONCEPT IS BEDOELD VOOR EEN NEDERLANDSE LEVERANCIER EN EEN NEDERLANDSE KLANT. EEN EU LEVERANCIER MOET QUA BEVEILIGING DE EISEN VAN DAT LAND NALEVEN. MET EEN NIET EU LEVERANCIER (OF ONDERAANNEMER) ZULLEN DIKWIJLS EU STANDARD CONTRACTUAL CLAUSES MOETEN WORDEN AANGEGAAN.

EEN AANTAL UITZONDERINGEN/BEPALINGEN IS REEDS TOEGEVOEGD N.A.V. DE VERORDENING DIE DE WBP MOET GAAN VERVANGEN EN VANAF 25 MEI 2018 MOET WORDEN NAGELEEFD. ONTWIKKELINGEN OP DIT VLAK MOETEN NAUWLETTEND IN DE GATEN WORDEN GEHOUDEN.

DE BLOKJES IN GEEL MOETEN IN IEDER GEVAL NOG WORDEN AANGEPAST/GEVERIFIEERD EN/OF BEVATTEN TOELICHTING

CONCEPT BEWERKERSOVEREENKOMST [- Bijlage bij Contract]

Deze overeenkomst (hierna te noemen de "**Bewerkersovereenkomst**") is aangegaan door:

1. […], hierna te noemen "**Klant**"; en

2. […], hierna te noemen "**Leverancier**";

Hierna gezamenlijk ook genoemd "Partijen" en afzonderlijk "Partij";

OVERWEGEN ALS VOLGT:

A. Klant gaat gebruik maken van de diensten van Leverancier […ˇ / zoals beschreven in het Contract tussen Partijen waarvan deze Bewerkersovereenkomst deel uitmaakt];

B. Leverancier verwerkt in het kader van deze dienstverlening in opdracht van en ten behoeve van Klant persoonsgegevens in de zin van de Wet bescherming persoonsgegevens (hierna "**Wbp**") waaronder van […**specificeer de persoonsgegevens en categorieën betrokkenen / kan worden gespecificeerd in Annex 1**];

C. Klant wenst uit hoofde van de verplichtingen die op een verantwoordelijke rusten in de zin van de Wbp, alsmede in het kader van beveiliging, bepaalde additionele waarborgen schriftelijk vast te leggen ten aanzien van het Verwerken van deze Persoonsgegevens en overige informatie door Leverancier;

KOMEN ALS VOLGT OVEREEN:

1. Begrippen Persoonsgegevens en Verwerken

De begrippen "Verwerken/Verwerking" hebben de betekenis van Verwerking zoals gedefinieerd in de Wbp. Persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. In deze Bewerkersovereenkomst is Persoonsgegeven gedefinieerd als elk gegeven betreffende een betrokkene waarvan persoonsgegevens worden Verwerkt waarvoor Klant als verantwoordelijke in de zin van de Wbp moet worden beschouwd en Leverancier als bewerker, waaronder […**specificeer de persoonsgegevens en categorieën betrokkenen / kan worden gespecificeerd in Annex 1**]. Dit betreft alle door Leverancier Verwerkte Persoonsgegevens, alsmede die Persoonsgegevens waarvan Leverancier anderszins kennis neemt, of kennis zou kunnen nemen in het kader van de in het Contract beschreven dienstverlening (een nadere beschrijving is opgenomen in Annex 1).

[**NB: De dienstverlening, de duur daarvan, doeleinden, persoonsgegevens en betrokkenen moeten zijn omschreven. Zie ook Annex 1. Als bewerker neemt Leverancier geen beslissingen over het gebruik van de Persoonsgegevens, de verstrekking aan derden en de duur van opslag van de Persoonsgegevens. Een leverancier die de rekening stuurt aan een (contactpersoon van een) Klant en of marketing informatie stuurt aan de Klant is daarvoor natuurlijk zelf verantwoordelijke.**]

2. Geheimhouding, doel Verwerking en instructies

2.1 Leverancier zal, en zal ervoor instaan dat een ieder die handelt onder zijn gezag (als gespecificeerd in Annex 1),[**NB: er zou volgens de Autoriteit Persoonsgegevens volgens de richtlijnen beveiliging d.d. februari 2013 omschreven moeten worden welke (groepen) medewerkers van leverancier toegang hebben tot welke persoonsgegevens en welke handelingen zij uit mogen voeren met de persoonsgegevens**]
a) de Persoonsgegevens en overige vertrouwelijke informatie waarvan zij kennis nemen geheimhouden, behoudens voor zover enig Nederlands of EU wettelijk voorschrift of wettelijk voorschrift van een EU lidstaat hen tot mededeling verplicht - in welk geval de Leverancier de Klant hierover onmiddellijk schriftelijk zal informeren tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt - of uit hun taak de noodzaak tot mededeling voortvloeit [**NB: wellicht is er een definitie van Vertrouwelijke Informatie in het Contract**];
b) de Persoonsgegevens slechts Verwerken in opdracht van en ten behoeve van Klant en voor zover noodzakelijk in het kader van de overeengekomen dienstverlening, behoudens voor zover enig Nederlands of EU wettelijk voorschrift of wettelijk voorschrift van een EU lidstaat hen

tot Verwerking verplicht - in welk geval de Leverancier de Klant hierover onmiddellijk schriftelijk zal informeren tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt, en alle schriftelijke instructies van Klant opvolgen; en

c) onverminderd hetgeen is bepaald onder 2.1b, de Persoonsgegevens niet (laten) Verwerken voor enig ander doel en geen andere handelingen met Persoonsgegevens uitvoeren dan overeengekomen in het kader van de dienstverlening.

2.2 Leverancier zal alle toepasselijke privacy wet- en regelgeving naleven waaronder de Wbp. Leverancier zal Klant onmiddellijk schriftelijk op de hoogte stellen indien de Leverancier van mening is dat een door de Klant gegeven instructie in strijd is met de Wbp en/of overige wet- en regelgeving.

3. Beveiliging

3.1 Leverancier zal passende technische en organisatorische maatregelen treffen in de zin van de Wbp teneinde de hiervoor genoemde Persoonsgegevens en overige vertrouwelijke informatie van Klant te beveiligen tegen verlies, of tegen enige vorm van onrechtmatige Verwerking. Deze maatregelen dienen, rekening houdend met de stand van de techniek, en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau te garanderen gelet op de risico's die de Verwerking en de aard van de Persoonsgegevens met zich meebrengen. De maatregelen dienen er mede op gericht te zijn onnodige verzameling en verdere Verwerking van Persoonsgegevens te voorkomen. Deze maatregelen zijn schriftelijk vastgelegd in Annex 2 en voldoen aan de richtlijnen van de Autoriteit Persoonsgegevens inzake beveiliging waaronder die van februari 2013. [**NB: deze richtlijnen bevatten ook een checklist wat in een bewerkersovereenkomst moet worden opgenomen**.]

3.2 Leverancier zal aanvullende maatregelen treffen op verzoek van Klant.

4. Audit

4.1 Leverancier stelt Klant in de gelegenheid de naleving van deze Bewerkersovereenkomst en wettelijke bepalingen die op de Verwerking van de Persoonsgegevens van toepassing zijn, periodiek te controleren. Leverancier zal daartoe onder meer de benodigde ruimte en gegevens toegankelijk maken en ter beschikking stellen en zal alle medewerking verlenen die redelijkerwijs kan worden gevraagd. De controle kan namens Klant worden uitgevoerd door een (externe) onafhankelijke auditor.

4.2 Indien uit een dergelijke controle blijkt dat Leverancier de Bewerkersovereenkomst en/of toepasselijke wettelijke bepalingen die op de Verwerking van Persoonsgegevens van toepassing zijn niet of niet geheel heeft nageleefd, dient Leverancier de kosten van het onderzoek voor zijn rekening te nemen. Ook zal Leverancier onverwijld na kennisneming van de geconstateerde tekortkomingen, deze tekortkomingen herstellen.

Leverancier zal zelf periodieke beveiligingsaudits uitvoeren en zal elk kwartaal een samenvatting verstrekken van de uitkomst van deze audits die minimaal een overzicht bevat van de risico's alsmede de maatregelen om deze te beperken en verhelpen. [**NB: Te specificeren in overleg met Leverancier.**]

5. Doorgifte buiten Nederland

Leverancier zal de hiervoor genoemde Persoonsgegevens slechts Verwerken in [Nederland / de Europese Unie] en geen toegang geven tot deze Persoonsgegevens aan, en/of deze Persoonsgegevens niet verstrekken aan, een ontvanger buiten [Nederland / de Europese Unie], tenzij Klant hier uitdrukkelijk vooraf schriftelijk mee heeft ingestemd, behoudens voor zover enig Nederlands of EU wettelijk voorschrift of wettelijk voorschrift van een EU lidstaat hen tot mededeling verplicht - in welk geval de Leverancier de Klant hierover onmiddellijk schriftelijk zal informeren tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.[**NB: uitzondering toegevoegd n.a.v. Verordening. Idem elders.**]

Het is uitsluitend ter keuze van Klant of hij deze toestemming verleent en/of welke eventuele voorwaarden hij verbindt aan deze toestemming.

6. Onderaanneming

6.1 Leverancier zal de uitvoering van de dienstverlening niet geheel en niet gedeeltelijk aan derden uitbesteden zonder voorafgaande schriftelijke toestemming van Klant. Klant heeft het recht deze toestemming zonder opgave van reden te weigeren of aan deze toestemming nadere voorwaarden te verbinden.

6.2 Indien Klant voor het uitbesteden toestemming verleent, is Leverancier hoofdelijk aansprakelijk voor de nakoming van de verplichtingen van diens onderaannemer. De bepalingen uit deze Bewerkersovereenkomst zullen minimaal ook door deze onderaannemer moeten worden nageleefd. Dit zal worden bepaald in de schriftelijke overeenkomst tussen Leverancier en de onderaannemer.

7. Medewerking en informatie

7.1 Leverancier zal Klant onverwijld en in ieder geval binnen [36 uur] op de hoogte stellen van:

a) een beveiligingsincident of datalek, of een schending van één van de andere verplichtingen als opgenomen in deze Bewerkersovereenkomst;
b) een klacht of verzoek (tot bijvoorbeeld inzage, correctie, aanvulling, verwijdering of afscherming) van een betrokkene waarvan Persoonsgegevens worden Verwerkt, en/of
c) een verzoek of bevel van, of onderzoek door, een toezichthouder of andere bevoegde autoriteit, voor zover dit is toegestaan ingevolge toepasselijke wet- en regelgeving.

7.2. Leverancier zal Klant onverwijld alle informatie verstrekken en medewerking verlenen waarom Klant verzoekt in het kader van de hierboven in artikel 7.1 onder a tot en met c genoemde situaties. [**NB Volgens de richtlijnen inzake beveiliging van de Autoriteit Persoonsgegevens (d.d. feb 2013) moeten worden opgenomen: afspraken over de inhoud van rapportages over beveiligingsincidenten en datalekken, de criteria voor rapportage van incidenten en de snelheid waarmee wordt gerapporteerd. Specificatie te bespreken met Leverancier.**] Leverancier zal aan Klant alle medewerking verlenen om de Klant in staat te stellen toepasselijke privacy wet- en regelgeving na te leven waaronder inzake het uitvoeren van een gegevensbeschermingseffectbeoordeling (data protection impact assessment) en/of naar aanleiding van (voorafgaande) raadpleging van een toezichthouder of andere bevoegde autoriteit. [**NB: N.a.v. Verordening**]

7.3. Indien deze Bewerkersovereenkomst en/of het Contract op welke wijze dan ook eindigt en/of op eerste verzoek van Klant, zal Leverancier: [**NB: Nog te specificeren hoe en in welke vorm en hoe kan worden zeker gesteld dat Leverancier geen toegang meer heeft.**]

(a) onmiddellijk ieder gebruik of andere Verwerking in de zin van de Wbp van de Persoonsgegevens staken; en
[**NB: Persoonsgegevens is uit te breiden met andere vertrouwelijke informatie, maar wellicht al ruime geheimhoudingsbepaling voor dit soort informatie in Contract, SLA, of algemene voorwaarden.]**

(b) in ieder geval binnen vijf (5) werkdagen ervoor zorgdragen dat alle documenten en/of andere informatiedragers die Persoonsgegevens bevatten en/of daarop betrekking hebben (waaronder alle kopieën in welke vorm dan ook) ter keuze van Klant (i) worden teruggeven aan Klant en/of (ii) op schriftelijk verzoek van Klant worden vernietigd, behoudens voor zover enig Nederlands of EU wettelijk voorschrift of wettelijk voorschrift van een EU lidstaat hen verplicht de Persoonsgegevens te bewaren - in welk geval de Leverancier de Klant hierover onmiddellijk schriftelijk zal informeren tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.[**NB: uitzondering toegevoegd n.a.v. Verordening. De duur van de verwerking moet duidelijk zijn en er moet ook niet worden vergeten een beroep te worden gedaan op 7.3b zodra de dienstverlening door Leverancier is geëindigd**].

7.4 Leverancier zal Klant schriftelijk informeren over relevante veranderingen met betrekking tot de dienstverlening. [**In Contract vastleggen dat dit reden kan zijn voor beëindiging Contract.**]

8. Overige

8.1 Leverancier zal de Persoonsgegevens gescheiden houden van gegevens die zij voor zichzelf of voor derden Verwerkt. **[NB: kan ook onderdeel uitmaken van Annex 2]**

8.2 In geval van tegenstrijdigheid tussen een bepaling van deze Bewerkersovereenkomst en een bepaling in een andere overeenkomst gesloten tussen Partijen (waaronder algemene voorwaarden), prevaleert de bepaling in deze Bewerkersovereenkomst. [**NB: Dit kan ook in het Contract worden opgelost in de tegenstrijdigheidsclausule.**]

8.3 Deze Bewerkersovereenkomst zal worden aangepast in onderling overleg tussen Klant en Leverancier indien dit is vereist ingevolge (toekomstige) toepasselijke wet- en regelgeving, of indien andere persoonsgegevens worden Verwerkt dan voorzien bij het aangaan van de Bewerkersovereenkomst. [**NB: Zoals bijv. door de Verordening die de Wbp moet vervangen etc.] [In het Contract verder ingaan op een noodplan indien bijv. een van de partijen de relatie wil beëindigen voor het einde van de contractperiode, een faillissement van partijen etc.]**

9. Toepasselijk recht en bevoegde rechter

Op deze Bewerkersovereenkomst is Nederlands recht van toepassing. De bevoegde rechter te […] is bij uitsluiting bevoegd om van alle geschillen die mochten ontstaan tussen Partijen voortvloeiende uit of in verband met (de uitvoering van) deze Bewerkersovereenkomst kennis te nemen.
[NB: Staat wellicht al in Contract? Daarbij aansluiten.]

Deze Bewerkersovereenkomst is ondertekend in tweevoud

Klant

_____

Naam:
Functie:
Datum:

Leverancier

_____

Naam:
Functie:
Datum:

Annex 1

1. Soort Persoonsgegevens en categorieën van betrokkenen:

[…]

2. Aard en doeleinden van de Verwerking / omschrijving van de dienst van Leverancier:

[…] **[NB: wellicht al duidelijk beschreven.]**

3. Welke (groepen) medewerkers van leverancier toegang hebben tot welke Persoonsgegevens en welke handelingen deze medewerkers uit mogen voeren met de Persoonsgegevens
[**NB: dit staat in de richtlijnen beveiliging van de Autoriteit Persoonsgegevens (d.d. februari 2013), maar kan ook volgen uit de beveiligingsmaatregelen of daarin zijn opgenomen.**]

Annex 2

Overzicht beveiligingsmaatregelen:

[…NB Zie ook de richtlijnen van de Autoriteit Persoonsgegevens]

Bijlage 4.b.: Bewerkersovereenkomst (met groepsvennootschap optie) ENG

THIS DRAFT CONTAINS STANDARD PROVISIONS AND HAS BEEN DRAWN UP IN CONSULTATION WITH NAUTADUTILH N.V.
PLEASE CONSULT YOUR LEGAL ADVISOR ON THE BASIS OF SPECIFIC CIRCUMSTANCES AND NEGOTIATIONS.

THIS DRAFT IS INTENDED FOR AN EU SUPPLIER AND A DUTCH CUSTOMER. FOR NON EU SUPPLIERS / SUBCONTRACTORS OF SUPPLIERS: EU STANDARD CONTRACTUAL CLAUSES OFTEN NEED TO BE ENTERED INTO.

A NUMBER OF PROVISIONS HAVE BEEN INCLUDED WITH A VIEW TO THE GENERAL DATA PROTECTION REGULATION WHICH NEEDS TO BE COMPLIED WITH AS OF 25 MAY 2018. DEVELOPMENTS IN THIS AREA SHOULD BE CLOSELY MONITORED.

THE PARTS IN YELLOW CONTAIN CHOICES OR AN EXPLANATION. FOR MORE EXPLANATIONS ALSO SEE THE DUTCH MODEL. THE ENGLISH AND DUTCH VERSIONS ARE NOT TRANSLATIONS, BUT DIFFERENT MODELS (ALTHOUGH SIMILAR TO A LARGE EXTENT).

THE DISCLAIMER AS INCLUDED IN THE 'STAPPENPLAN' ALSO APPLIES TO THIS DRAFT DATA PROCESSING AGREEMENT.

DRAFT DATA PROCESSING AGREEMENT [- Appendix to Agreement]

THE UNDERSIGNED

1. [**Name Customer**], a company organised under the laws of the Netherlands, whose corporate seat is at […], the Netherlands; hereinafter referred to as "Customer"; and

2. [**Name supplier**], a company organised under the laws of […], whose corporate seat is at [municipality, country]; hereinafter referred to as "Supplier";

WHEREAS

1. Supplier shall deliver certain services to Customer [and/or its group companies] namely [**describe services**] (hereafter "**Services**");

2. Customer [and/or its group companies] need[/s] to comply with data protection legislation and wish[es] to have Supplier secure certain data and therefore Customer wishes to enter into this Data Processing Agreement with Supplier;

NOW HEREBY AGREE AS FOLLOWS

1. Meaning of terms Personal Data and Processing

The expression "**Process/Processing**" shall have the meaning given to it in the Personal Data Protection Act (*Wet bescherming persoonsgegevens*) and/or other applicable data protection legislation. Personal data shall mean any information relating to an identified or identifiable natural person. In this Data Processing Agreement **Personal Data** is defined as any information relating to [**describe categories of personal data and categories of data subjects or include in Annex 1**].

2. Processing of Personal Data

2.1 Supplier and the persons acting under its authority (as specified in **Annex 1**) shall only Process such Personal Data insofar as necessary for the performance of the Services and shall only Process such Personal Data by order of and for Customer [and/or any of its group companies] and in accordance with its[/their] [written][**FYI: the instructions should be documented according to the General Data Protection Regulation**] instructions, subject to EU or EU member state statutory provisions to the contrary in which case Supplier shall inform the Customer of such legal requirement before Processing the Personal Data unless such law prohibits such information on important grounds of public interest. Supplier is not allowed to Process the Personal Data for any other purpose and acts as a data processor (*bewerker*) as defined in the Personal Data Protection Act. Supplier shall immediately inform Customer if, in Supplier's opinion, an instruction breaches EU or EU member state data protection provisions.

2.2 Supplier shall comply with all applicable data protection laws, rules and regulations including but not limited to the Personal Data Protection Act (insofar as applicable). [**FYI: A supplier in another EU country should comply with the security requirements according to that country**]

3. Security measures

3.1 Supplier warrants it has taken and shall at all times take all appropriate technical and organisational measures to secure the Personal Data and all other information accessed and/or otherwise Processed by Supplier on behalf of Customer [and/or its group companies] including Confidential Information [**FYI: this can be included if there is a definition in the Agreement**] against unauthorised access, loss or any form of unlawful Processing and shall comply with applicable data protection laws, rules and regulations, by taking among other things the measures set out in **annex 2** [**FYI: please attach the Supplier's written Security Policy and ensure it is in conformity with the data protection authority's guidelines**]. Supplier shall warrant an appropriate level of security, taking into account the state of the art and the costs of implementation, and having regard to the risks associated with the Processing and the nature of the data to be protected. The measures shall also aim at preventing unnecessary collection and further Processing of Personal Data.

Notwithstanding Article 3.1, Supplier shall comply with any security requirements expressly required by Customer such as are reasonably necessary to comply with applicable laws, rules and regulations.

4. Audit

4.1 Customer [and/or its group companies] is[/are] entitled to periodically inspect compliance with the Data Processing Agreement (including the security measures taken) [also on behalf of its group companies]. Customer [and/or its group companies] may contract out this inspection to an external independent auditor. If it emerges from such an inspection that Supplier failed to comply or properly comply, in whole or in part, with the Data Processing Agreement and/or any applicable laws, rules and regulations, Supplier must bear the costs of such investigation. Supplier shall make available all information necessary to demonstrate compliance with its obligations and shall provide all reasonable assistance.

4.2 Supplier shall perform regular security checks and shall provide quarterly summaries of the outcome of such checks which minimally contain an overview of risks, measures taken to mitigate and remedy such risks, and updates implemented.

5. Transfer/access outside the European Union

Supplier shall only Process Personal Data within the European Union and shall not grant access to or transfer Personal Data (or any other information Processed by Supplier on behalf of Customer [and/or its group companies]) to a recipient located in a country outside the European Union, unless Customer consented to this in writing prior to such access or transfer. Customer may, at its sole discretion, provide such written consent subject to the fulfilment of further conditions.
This obligation is subject to EU or EU member state statutory provisions to the contrary in which case Supplier shall inform the Customer of such legal requirement before granting access to or transferring Personal Data unless such law prohibits such information on important grounds of public interest.

6. Subcontracting

6.1 Supplier shall not use any subcontractor(s) unless Customer has given its prior written approval of such subcontracting. Supplier shall remain fully and unconditionally liable for the performance by any subcontractor of the obligations or parts of it arising out of any agreement between Customer [and/or its group companies] and Supplier.

6.2 Supplier shall also prior to using any subcontractor(s) enter into a written agreement with such subcontractor which obliges this subcontractor to comply with all obligations imposed on the Supplier in this Data Processing Agreement.

7. Confidentiality

7.1 Anyone acting under the authority of the Supplier, as well as the Supplier itself, where they have access to Personal Data, may only Process such Personal Data if they are required to treat as confidential the Personal Data which comes to their knowledge, except where the communication of such Personal Data is required by the proper performance of their duties or EU or EU member state law to which Supplier is subject in which case Supplier shall inform the Customer of such legal requirement before communicating the Personal Data unless such law prohibits such information on important grounds of public interest.

7.2 All Personal Data and all other information provided by Customer [and/or its group companies] including all copies in whatever form in the Supplier's possession or control shall further and according to the instructions of Customer at the Customer's choice either be i) destroyed, or ii) returned to Customer [and/or its group companies], upon the Customer's first request, unless EU or EU member state law require Supplier to store the data in which case Supplier shall inform the Customer of such legal requirement unless such law prohibits such information on important grounds of public interest.

8. Miscellaneous

8.1 Supplier shall keep the Personal Data logically separate to data Processed on behalf of any other third party and from its own data. [**FYI: This can be part of Annex 2**]

8.2 Supplier shall grant applicable supervisory authorities and other competent authorities where such authorities have the legal right to carry out an investigation of Customer's [and/or its group companies'] or Supplier's Processing activities, such access to its premises, computer and other information systems and records as may be reasonably required.

8.3 Supplier shall implement appropriate procedures and any associated measures that will ensure that Customer's [and/or its group companies'] instructions can be complied with, including but not limited to comply with any request of a data subject to access, correct, supplement, delete or block Personal Data. Supplier shall assist Customer, where necessary and upon Customer's first request, in ensuring compliance with any data protection obligations including but not limited to deriving from the carrying out of a data protection impact assessment and from prior consultation of a supervisory or other competent authority.

8.4 Supplier shall notify Customer immediately of, and provide details of:
i) any known breach of its technical and/or organisational security measures, any possible Personal Data leakage, loss, unauthorised access, or any form of unlawful Processing, any known breach of confidentiality obligations or any other violation of applicable data protection laws, rules and regulations, as well as a) cooperate with Customer [and/or its group companies] upon such company's first request to provide adequate information to data subjects and b) include in such report all details which allow Customer [and/or its

group companies] to comply with the Personal Data Protection Act and/or other applicable data protection laws, rules and regulations and provide all information which Customer [and/or its group companies] request[s];
ii) any investigation of any supervisory authority or other competent authority insofar as this is allowed pursuant to applicable laws, rules and regulations; and/or
iii) any complaint, question, or request of a data subject whose Personal Data are Processed.

8.5 In the event of a conflict between a provision in this Data Processing Agreement and a provision in any other agreement between Customer [and/or its group companies] and Supplier (including any general terms and conditions), the provision in the Data Processing Agreement shall prevail.

8.6 This Data Processing Agreement shall be governed by and construed in accordance with Dutch law. Any dispute arising in connection with this Data Processing Agreement shall be submitted to the exclusive jurisdiction of the competent court in Amsterdam, the Netherlands.

8.7 Customer may amend this Data Processing Agreement if reasonably required to comply with applicable laws, rules and regulations or by change in the Personal Data Processed.

AGREED by the Parties' following authorised representatives

For and on behalf of Customer	For and on behalf of Supplier
_____(Signature)	_____(Signature)
Name:	Name:
Title:	Title:
Date:	Date:

Annex 1

1. Categories of Personal Data and Categories of data subjects:

[…]

2. Nature and purposes of Processing / description of service of Supplier:

[…]

3. Which employees or groups of employees of Supplier have access to which Personal Data and which activities can these staff members perform with the Personal Data:

[…]

Annex 2

[**Overview of security measures; there are guidelines from the data protection authority with respect to the security measures which need to be taken**]

Bijlage 5: Voorbeeld Protocol meldplicht datalekken [organisatie]

Versie 2.0 d.d. 22 december 2015

1. Inleiding

Per 1 januari 2016 geldt ingevolge de Wet bescherming persoonsgegevens (“Wbp”) een meldplicht datalekken. Om aan de verplichtingen uit deze wet te voldoen heeft [organisatie] dit protocol vastgesteld.

Volgens de Wbp dient de Autoriteit Persoonsgegevens onverwijld in kennis te worden gesteld van een ‘inbreuk op de beveiliging van persoonsgegevens' die 'leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens’. In dit protocol wordt een dergelijk incident aangeduid als een “Datalek”.

De betrokkene (de persoon op wie de gegevens betrekking hebben) dient daarnaast onverwijld in kennis te worden gesteld van de inbreuk indien de inbreuk ‘waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer’.

De Autoriteit Persoonsgegevens heeft beleidsregels meldplicht datalekken vastgesteld (“Beleidsregels”) aan de hand waarvan organisaties kunnen bepalen wanneer de meldplicht van toepassing is.

Melding dient volgens de wet onverwijld plaats te vinden. Volgens de Beleidsregels dient melding aan de Autoriteit Persoonsgegevens plaats te vinden binnen 72 uur.

De wet stelt zware sancties op overtreding van de meldplicht. Het is daarom van belang dat dit protocol strikt wordt nageleefd.

[Naam contactpersoon] (hierna: “de Contactpersoon”) draagt binnen onze organisatie zorg voor de naleving van de meldplicht. Het is in geval van mogelijke Datalekken van belang [naam contactpersoon] direct te informeren, zodat de Contactpersoon de situatie kan beoordelen en de nodige acties in gang kan zetten. [Daarnaast eventueel melding aan bijvoorbeeld ICT, management]

2. Wanneer kan er een meldplicht zijn

De Autoriteit Persoonsgegevens gaat uit van een ruime lezing van het begrip Datalek. Hiervan kan sprake zijn wanneer persoonsgegevens in verkeerde handen komen, verloren gaan, niet langer meer toegankelijk zijn voor de verantwoordelijke, er sprake is van een onrechtmatige inzage of wanneer er een onrechtmatige verwerking plaats vindt.

Een aantal concrete voorbeelden van een Datalek is:

- het verlies van een niet-versleutelde USB-stick of DVD, laptop, telefoon of tablet met daarop persoonsgegevens;
- onrechtmatige toegang tot een personeelsdossier;
- een inbraak door een hacker;
- verloren gaan van persoonsgegevens door een calamiteit (bijvoorbeeld een brand of een menselijke fout, zoals het per ongeluk wissen van bestanden) zonder dat er een deugdelijke back-up is gemaakt;

- het slachtoffer worden van een ransomware-uitbraak waardoor gegevens niet meer toegankelijk zijn.

Ga er bij twijfel van uit dat sprake is van een Datalek zodat er een (interne) melding moet worden gedaan.

3. Ieder mogelijk Datalek direct intern melden

Ieder Datalek dient direct en met hoge prioriteit gemeld te worden aan de Contactpersoon.

Voorzie de Contactpersoon van zoveel mogelijk relevante gegevens, zoals een korte beschrijving van wat er is gebeurd, datum en tijdstip, een schatting van het aantal betrokken natuurlijke personen, soorten gegevens, en mogelijke gevolgen voor de betrokken personen. Dit kan later overigens worden aangevuld, vanwege de korte termijnen is het van belang om vooral te zorgen dat de Contactpersoon snel op de hoogte is. Controleer of de Contactpersoon ook daadwerkelijk van de e-mail kennis heeft genomen. Bij afwezigheid van de Contactpersoon dient mede contact te worden gezocht met [gegevens vervanger(s)].

4. Wat gebeurt er met de interne melding

De Contactpersoon zal aan de hand van de Wbp, de Beleidsregels en eventueel in overleg met het management, [ICT] en / of externe adviseurs beoordelen of melding aan de Autoriteit Persoonsgegevens en / of aan betrokkene(n) dient plaats te vinden. Als het nodig is het Datalek aan de Autoriteit Persoonsgegevens te melden, dan zal de Contactpersoon deze melding doen.

Ook zal de Contactpersoon, eventueel in overleg met het management, [ICT], [communicatie] en / of externe adviseurs beoordelen of andere maatregelen genomen dienen te worden, zoals aangifte bij de politie, melding bij de verzekeraar, schadebeperkende maatregelen zoals (indien mogelijk) van afstand wissen van gegevens (‘remote wiping’), wijziging van wachtwoorden, aanvullende beveiligingsmaatregelen, of maatregelen op het gebied van communicatie.

Indien melding aan de Autoriteit Persoonsgegevens plaatsvindt zullen gegevens over het incident tevens vastgelegd en bewaard dienen te worden.

5. Overeenkomsten met bewerkers

Indien onze organisatie een derde inschakelt om in opdracht persoonsgegevens te verwerken (“bewerker”), blijft onze organisatie verantwoordelijk voor de naleving van de verplichtingen uit de Wbp. Dit dient te worden vastgelegd in een schriftelijke overeenkomst, de bewerkersovereenkomst. Met het oog op de Meldplicht Datalekken dient de bewerkersovereenkomst vanaf 1 januari 2016 onder meer een regeling te bevatten over de wijze waarop aan de Meldplicht Datalekken wordt voldaan. Alle bewerkersovereenkomsten moeten worden gesloten volgens het meest actuele model dat [organisatie] hiervoor hanteert. Eventuele bewerkersovereenkomsten die nog niet voldoen aan de per 1 januari 2016 geldende standaarden, moeten worden aangepast.

6. Vragen

Voor vragen over de meldplicht Datalekken kunt u zich wenden tot [naam contactpersoon].

[contactgegevens]