Privacyreglement SWV Helmond-Peelland VO

Artikel 1 Begrippen

Voor de toepassing van dit reglement en de daarbij behorende bijlage(n) en instructie(s) wordt verstaan onder:

a. Directeur: persoon die door het bestuur is benoemd tot directeur van het bureau van stichting SWV Helmond-Peelland VO;
b. AP: Autoriteit Persoonsgegevens, de toezichthouder op de naleving van de wet bescherming persoonsgegevens; voorheen het College Bescherming Persoonsgegevens;
c. Beheerder: degene die namens het bestuur verantwoordelijk is voor de dagelijkse zorg voor de verwerking, voor de juistheid van de ingevoerde gegevens, voor het bewaren, verwijderen en verstrekken van gegevens;
d. Bestand: elk gestructureerd geheel van persoonsgegevens ongeacht of dit geheel van gegevens gecentraliseerd of verspreid is op functioneel of geografisch bepaalde wijze dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen;
e. Betrokkene: degene op wie een persoonsgegeven betrekking heeft (waaronder personeel en leerlingen);
f. Bewerker: degenen die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;
g. Bewerkersovereenkomst: de overeenkomst die met een bewerker wordt gesloten om te komen tot een duidelijke verwerking van persoonsgegevens;
h. Bijzondere persoonsgegevens: persoonsgegevens als bedoeld in artikel 16 van de Wbp. Dit zijn gegevens over: godsdienst, levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging, strafrechtelijke gegevens, onrechtmatig of hinderlijk gedrag in relatie met een opgelegd verbod naar aanleiding van dat gedrag;
i. Bureau: SWV Helmond-Peelland VO;
j. Datalek: inbreuk op de beveiliging van persoonsgegevens zoals bedoeld in artikel 13 Wbp, waardoor de persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking.
k. Derde: ieder, niet zijnde betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is persoonsgegevens te verwerken;
l. FG: Functionaris Gegevensbescherming: ook wel de vertegenwoordiger. Degene die namens het bestuur bevoegd is datalekken te melden bij de AP en ook als zodanig staat ingeschreven in het register van FG-functionarissen;
m. Gebruiker: degene die gerechtigd is kennis te nemen van bepaalde gegevens in de persoonsregistratie;
n. Leerling: persoon die zich schriftelijk heeft aangemeld om onderwijs te volgen of onderwijs volgt op een van de aangesloten scholen van SWV Helmond-Peelland VO of persoon die zich elders bij een school schriftelijk heeft aangemeld om onderwijs te volgen of onderwijs volgt maar wel tot de doelgroep van SWV Helmond-Peelland VO gerekend mag worden;
o. Ontvanger: degene aan wie de persoonsgegevens (kunnen) worden verstrekt;
p. Personeel: personen in dienst van of werkzaam ten behoeve van SWV Helmond-Peelland VO;
q. Persoonsgegevens: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;
r. Bestuur: bestuur en bevoegd gezag van SWV Helmond-Peelland VO;
s. Reglement: dit reglement inclusief bijlagen;
t. SWV Helmond-Peelland VO: stichting Samenwerkingsverband Helmond-Peelland vo en vso.
u. Toestemming van de betrokkene: elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt;
v. Verantwoordelijke: bestuur van SWV Helmond-Peelland VO;
w. Verstrekken van persoonsgegevens: het bekend maken of ter beschikking stellen van persoonsgegevens;

x. Vertegenwoordiger: de FG;
y. Verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen (dat wil zeggen verkrijgen), vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van ter beschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;
z. Vrijstellingsbesluit Wbp: besluit van 7 mei 2001, houdende aanwijzing van verwerking van persoonsgegevens die zijn vrijgesteld van de melding bedoeld in artikel 27 van de Wbp;
aa. Wbp: Wet bescherming persoonsgegevens.

Artikel 2 Reikwijdte en doelstelling van het reglement

a. Dit reglement is van toepassing op alle persoonsgegevens betreffende het personeel en de leerlingen van dan wel andere betrokkenen die door of namens het bestuur van de stichting SWV Helmond-Peelland VO worden verwerkt.
b. Dit reglement heeft tot doel:
   1. de persoonlijke levenssfeer van betrokkenen van wie persoonsgegevens worden verwerkt te beschermen tegen misbruik van die gegevens en tegen het verwerken van onjuiste gegevens;
   2. te voorkomen dat persoonsgegevens worden verwerkt voor een ander doel dan het doel waarvoor ze verzameld zijn.

Artikel 3 Verwerking van persoonsgegevens overeenkomstig het doel waarvoor ze zijn verkregen

1. Slechts die persoonsgegevens mogen worden verzameld en (verder) verwerkt , die rechtmatig verkregen zijn en waarvoor een rechtmatige grondslag bestaat.
2. De in lid 1 vermelde grondslag kan worden gebaseerd op een van de volgende gevallen:
   a. de verwerking is noodzakelijk voor de uitvoering van een overeenkomst (bijvoorbeeld arbeidsovereenkomst) waarbij de betrokkene partij is;
   b. de verwerking is noodzakelijk voor het gerechtvaardigde belang van de stichting SWV Helmond-Peelland VO;
   c. de verwerking is noodzakelijk om een wettelijke verplichting van de stichting SWV Helmond-Peelland VO na te kunnen komen;
   d. de verwerking is noodzakelijk ter vrijwaring van een vitaal belang van de betrokkene;
   e. de betrokkene heeft ondubbelzinnige toestemming voor de verwerking verleend.
3. De te verwerken persoonsgegevens worden slechts verder verwerkt op een wijze die verenigbaar is met het doel waarvoor ze zijn verkregen. De verwerking moet toereikend en noodzakelijk zijn voor het doel waarvoor ze zijn verkregen. Daarbij wordt tenminste rekeninggehouden met de verwantschap van de doelen, de aard van de gegevens, de gevolgen van de verdere verwerking voor de betrokkene, de wijzen waarop de gegevens zijn verkregen en de waarborgen ter bescherming van de persoonlijke levenssfeer.
4. Verwerking geschiedt ten behoeve van de volgende doeleinden:
   a. de organisatie van en het geven van onderwijsondersteuning en begeleiding van leerlingen;
   b. leerlingenadministratie;
   c. personeelsinformatie(systeem) en salarisadministratie voor het bureau;
   d. administratie ten behoeve van de bedrijfsvoering van SWV Helmond-Peelland VO;
   e. geschillenafhandeling en klachtbehandeling conform de verschillende bestaande reglementen en klachtenregelingen van SWV Helmond-Peelland VO;
   f. het doen uitoefenen van een accountantscontrole;
   g. de uitvoering of toepassing van een wettelijke regeling.

5. Er zijn wettelijke uitzonderingen op het principe ‘verenigbaar’ zoals vermeld in lid 3. De beheerder mag ook verwerken, indien dit noodzakelijk is in het belang van :
   a. de veiligheid van de staat;
   b. de voorkoming, opsporing en vervolging van strafbare feiten;
   c. gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
   d. het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de belangen bedoeld onder b en c;
   e. de bescherming van de betrokkenen of van de rechten en vrijheden van anderen.
6. Indien gegevens in een voorkomend geval op basis van een wettelijke uitzondering worden gebruikt, zal de verantwoordelijke zich over dat gebruik moeten verantwoorden. Hiervoor wordt vastgelegd welke gegevens van elke betrokken op welke wijze werden verwerkt, om welke wettelijke uitzonderingsgrond het ging en wat het specifieke doel voor de verwerking was. Op verzoek van de betrokken zal de verantwoordelijke hier inzicht in moeten verschaffen, tenzij het belang van een uitzonderingsgrond zicht hiertegen verzet.

Artikel 4 Verstrekken van persoonsgegevens

1. Het verstrekken van persoonsgegevens aan derden wordt gezien als een vorm van verwerking.
2. Het verstrekken va persoonsgegevens kan allen gebeuren indien:
   a. de verwerking noodzakelijk is voor de uitvoering van een overeenkomst (bijvoorbeeld arbeidsovereenkomst) waarbij de betrokkene partij is;
   b. de verwerking noodzakelijk is voor het gerechtvaardigde belang van het SWV Helmond-Peelland VO;
   c. de verwerking noodzakelijk is om een wettelijke verplichting van SWV Helmond-Peelland VO na te kunnen komen;
   d. de verwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;
   e. de betrokkene ondubbelzinnig toestemming voor de verwerking heeft verleend.

Artikel 5 Melding aan het AP

1. Voor melding van het AP komen die persoonsgegevens in aanmerking die geheel of gedeeltelijk geautomatiseerd worden verwerkt en die voor de verwezenlijking van een doeleinde of verschillende samenhangende doeleinden zijn bestemd, met uitzondering van de persoonsgegevens die niet geautomatiseerd worden verwerkt. Voor deze laatste categorie geldt dat de verwerking uitsluitende dient te worden gemeld indien de melding is onderworpen aan een voorafgaand onderzoek.
2. De melding dient voorafgaand aan de verwerking plaats te vinden.
3. De melding behelst een opgave van:
   a. De naam en het adres van de verantwoordelijke;
   b. het doel of de doeleinden van de gegevensbewerking;
   c. een beschrijving van de categorieën van betrokkenen en van de gegevens of categorieën van gegevens die daarop betrekking hebben;
   d. de ontvangers of categorieën van ontvangers aan wie de gegevens kunnen worden verstrekt;
   e. de voorgenomen doorgiften van gegevens naar landen buiten de Europese Unie;
   f. een algemene beschrijving van de te nemen beveiligingsmaatregelen.
4. De melding behelst het doel of de doeleinden waarvoor de gegeven of de categorieën van gegevens zijn of worden verzameld.

Artikel 6 Vrijstelling

Gegevensverwerkingen waarvan algemeen bekend is dat zij plaatsvinden en waarvan het onwaarschijnlijk is dat de persoonlijke levenssfeer van de betrokkenen door die verwerking wordt geschaad, zijn vrijgesteld van meldingsplicht. De voor het SWV

Helmond-Peelland VO geldende vrijstellingen zijn opgenomen in bijlage 2. Het betreft in ieder geval:

a. verwerking door de stichting SWV Helmond-Peelland VO met betrekking tot hun leden en begunstigers;
b. verwerkingen met betrekking tot sollicitanten;
c. verwerkingen in het kader van de personeelsadministratie en de salarisadministratie;
d. verwerkingen met betrekking tot debiteuren en crediteuren en verwerkingen met betrekking tot afnemers en leveranciers;
e. verwerkingen met betrekking tot leerlingen;
f. verwerkgingen ten dienste van het interne beheer van de organisatie van de verantwoordelijke, zoals verwerkingen met betrekking tot netwerk- en computersystemen, communicatieapparatuur en toegangscontrole.

Artikel 7 Persoonsgegevens

1. De persoonsgegevens moeten behoorlijk en zorgvuldig worden verwerkt in overeenstemming met de Wbp.
2. De persoonsgegevens worden verwerkt voor zover zij voor de geformuleerde doeleinden toereikend, ter zake dienend en niet bovenmatig zijn.
3. Welke persoonsgegevens mogen worden verwerkt, is opgenomen in de artikelen uit het Vrijstellingsbesluit Wbp, waarnaar in bijlage 2 wordt verwezen.
4. Bijzondere persoonsgegevens worden slechts verwerkt met inachtneming van de bepalingen in de artikelen 26 – 23 Wbp.
5. De beheerder treft de nodige voorzieningen ter bevordering van de juistheid en de volledigheid van de persoonsgegevens.

Artikel 8 Bewaartermijnen

1. Persoonsgegevens die niet langer voor het geformuleerde doel noodzakelijk zijn, worden zo spoedig mogelijk verwijderd.
2. In de selectielijst is opgenomen waar en in welke bescheiden moeten worden bewaard.
3. In de selectielijst is per bescheiden een vernietigingstermijn opgenomen.

Artikel 9 Beheer

1. Het bestuur is verantwoordelijk voor de diverse verwerkingen. De beheerder zorgt, namens het bestuur, voor het nakomen van de verplichtingen uit de Wbp.
2. De directeur van het bureau is beheerder van de verwerkingen van de persoonsgegevens die in zijn organisatie plaatsvinden.
3. De beheerder verwerkt overeenkomstig de in het reglement opgenomen richtlijnen en zorgt ervoor dat deze bekend zijn bij de gebruikers, bewerkers en derde.

Artikel 10 Bewerkersovereenkomst

1. Bij het inschakelen van een bewerker wordt een bewerkersovereenkomst afgesloten waarin wordt vastgelegd dat deze bewerker voldoende waarborgen biedt ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen.
2. In de bewerkersovereenkomst worden minimaal de vereisten uit artikel 14 lid 3 Wbp vastgelegd.

Artikel 11 Toegang

1. Behoudens daartoe strekkende voorschriften in wet- en regelgeving hebben slechts toegang tot de persoonsgegevens:
   a. Degenen, onder wie begrepen derden, die belast zijn met of leiding geven aan de activiteiten die in verband staan met de verwerking van gegevens of de daarbij noodzakelijk zijn betrokken;
   b. anderen, in de gevallen zoals bedoeld in artikel 8 onder a, c en d en artikel 9 lid 3 van de Wbp.
2. Onder lid 1 sub a van dit artikel vallen in ieder geval de verantwoordelijke, de beheerder zoals genoemd in artikel 8 lid 2 en de door de beheerder aangewezen gebruikers, bewerkers voor de persoonsgegevens over de tot hun werkgebied behorende betrokkenen.

Artikel 12 Beveiliging en geheimhouding

1. De verantwoordelijke draagt zorg voor passende technische en organisatorische maatregelen ter voorkoming van verlies of onrechtmatige verwerking van persoonsgegevens. Deze maatregelen garanderen, rekeninghoudend met de technische mogelijkheden en de kosten van de tenuitvoerlegging, een adequaat beveiligingsniveau, gelet op de risico's die de verwerking en de aard van de te beschermen persoonsgegevens met zich meebrengen. Deze maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.
2. Gelijke plicht rust op beheerder, gebruiker, bewerker en derde.
3. Indien sprake is van elektronische gegevensverwerking, zal de beheerder zorgdragen voor een coderingsbeveiliging waarbij de toegang van gebruikers, bewerkers en eventuele andere, door de beheerder aangewezen personen tot (bepaalde) persoonsgegevens wordt beperkt tot die gegevens, die noodzakelijk zijn et het oog op de door hen uit te voeren werkzaamheden.
4. Een ieder die betrokken is bij de uitvoering van dit reglement en daarbij de beschikking krijgt over persoonsgegevens waarvan hij het vertrouwelijk karakter kent of redelijkerwijs kan vermoeden en voor wie niet reeds uit hoofde van beroep, functie of wettelijk voorschrift ter zake van de persoonsgegevens een geheimhoudingsplicht geldt, is verplicht tot geheimhouding daarvan. Dit geldt niet indien enig wettelijk voorschrift hem tot bekendmaking verplicht of uit zijn taak bij de uitvoering van dit reglement de noodzaak tot bekendmaking voortvloeit.
5. Ingeval van technische werkzaamheden, die verband houden met onderhoud of reparatie van apparatuur en programmatuur, worden de persoonsgegevens zo veel mogelijk afgeschermd.
6. Indien gebruik wordt gemaakt van de diensten van een bewerker, worden door of namens de verantwoordelijke de wederzijdse verplichtingen met betrekking tot de beveiliging met persoonsgegevens schriftelijke in een overeenkomst met bewerker vastgelegd, zoals bepaald in artikel 9 van dit reglement.

Artikel 13 Datalekken

1. Bij een inbreuk op de beveiliging, zoals bedoeld in artikel 13 Wbp, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens wordt er melding gedaan bij de Functionaris Gegevensbescherming (FG) op het bureau van Stichting SWV Helmond-Peelland VO.
2. De FG onderzoekt of er sprake is van een datalek zoals bedoeld in artikel 34a Wbp en meldt dit onverwijld aan de AP conform het protocol datalekken.

Artikel 14 Recht op informatie

1. Indien het bestuur en/of het bureau van de betrokkene zelf persoonsgegevens krijgt, wordt voorafgaand aan die verkrijging de identiteit en het doel van die verwerking meegedeeld.
2. Indien het bestuur en/of het bureau persoonsgegevens van een derde of door observatie (bijvoorbeeld videocamerasysteem) van de betrokkene verkrijgt, informeert de beheerder de betrokkene op het moment van vastlegging.
3. Als de van de derde of door observatie verkregen gegevens bestemd zijn om te worden verstrekt aan een derde, informeert de beheerder de betrokkene uiterlijk op het moment van de eerste verstrekking.
4. In de hiervoor genoemde gevallen hoeft de betrokkene niet te worden geïnformeerd:
   a. Als deze hiervan reeds op de hoogte is;
   b. Indien mededeling aan de betrokkene onmogelijk blijkt of een onevenredige inspanning kost. In dat geval wordt de herkomst van de gegevens vastgelegd;
   c. In geval van een ander zwaarwegend belang, bijvoorbeeld wanneer het noodzakelijk is strafbare feiten te voorkomen, en de rechten en vrijheden van anderen te beschermen.

Artikel 15 Recht op inzage

1. Iedere betrokken heeft het recht op inzage te vragen. Een dergelijk verzoek tot inzage dient schriftelijk te worden gedaan aan de beheerder.
2. De beheerder deelt een ieder op diens verzoek, zo spoedig mogelijk, maar uiterlijk binnen vier weken na ontvangst van het verzoek, schriftelijk mee of door hem betreffende persoonsgegevens worden verwerkt.
3. Indien dat het geval is, verstrekt de beheerder de verzoeker desgewenst, zo spoedig mogelijk, maar uiterlijk binnen vier weken na ontvangst van het verzoek, schriftelijk een volledig overzicht daarvan met informatie over het doel van de verwerking, de categorieën van gegevens, de (categorieën van) ontvangers en de beschikbare informatie over herkomst van de gegevens. Desgewenst, informeert de beheerder de verzoeker over de systematiek van de geautomatiseerde verwerking.
4. Indien een derde naar verwachting bedenkingen tegen inzage zal hebben, wordt die derde in de gelegenheid gesteld om zijn zienswijze naar voren te brengen. Deze handelswijze hoeft echter niet indien dit onmogelijk is of een onevenredige inspanning kost.
5. Indien een gewichtig belang van de verzoeker dit eist, voldoet de beheerder aan het verzoek in een andere dan schriftelijke vorm, die aan dat belang is aangepast.
6. De beheerder draagt zorg voor een deugdelijke vaststelling van de identiteit van de verzoeker. Indien de beheerder twijfelt aan de identiteit van de verzoeker, vraagt hij zo spoedig mogelijk aan de verzoeker schriftelijk nadere gegevens inzake zijn identiteit te verstrekken of een geldig identiteitsbewijs te overleggen. Door dit verzoek wordt de termijn opgeschort tot het tijdstip dat het bewijs is geleverd.
7. Een verzoek om inzage kan kosteloos worden gedaan.
8. Een verzoek tot inzage kan worden geweigerd, indien het noodzakelijk is in het belang van:
   a. de veiligheid van de staat;
   b. de voorkoming, opsporing en vervolging van strafbare feiten;
   c. gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
   d. het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de belangen bedoeld onder b en c;
   e. de bescherming van de betrokkene of van de rechten en vrijheden van anderen.
9. Indien een verzoek tot inzage wordt geweigerd, dient dit gemotiveerd te worden door de beheerder. Uit de motivering moet blijken dat een zorgvuldige belangenafweging heeft plaatsgevonden van alle betrokken partijen.

Artikel 16 Recht op verbetering, aanvulling, verwijdering en/of afscherming

1. De betrokkene die op verzoek inzage heeft gekregen in de hem betreffende persoonsgegevens, kan de beheerder schriftelijk verzoeken de persoonsgegevens te verbeteren, aan te vullen te verwijderen, of af te schermen indien deze gegevens feitelijk onjuist zijn, voor het doel van de verwerking onvolledig of niet ter zake dienend dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt.
2. Het verzoek bevat de aan te brengen wijzigingen.
3. De beheerder deelt de verzoeker zo spoedig mogelijk, maar uiterlijk binnen vier weken na ontvangst van het verzoek, schriftelijk mee of hij daaraan voldoet. Indien hij daaraan niet of niet geheel wil voldoen, motiveert hij dat besluit.
4. De beheerder zorgt ervoor dat een beslissing tot verbetering, aanvulling, verwijdering en/of afscherming
5. Indien de gegevens zijn vastgelegd in een document of op een (andere) gegevensdrager waarin geen wijzigingen kunnen worden aangebracht, worden de onjuistheid en de aan te brengen wijzigingen in een afzonderlijk document opgenomen dat aan het dossier wordt toegevoegd. De verzoeker wordt hiervan in kennis gesteld.

6. De beheerder informeert in geval van verbetering, aanvulling, verwijdering of afscherming, de derden die eerder de betreffende gegevens hebben ontvangen, tenzij dit onmogelijk is of een onevenredige inspanning kost.
7. De beheerder deelt desgevraagd de verzoeker mee aan welke derden hij de hiervoor bedoelde mededeling heeft gedaan.

Artikel 17 Bezwaar/Recht van verzet

1. Indien de rechtmatige grondslag voor een bepaalde verwerking is gelegen in het gerechtvaardigde belang van de Stichting SWV Helmond-Peelland VO of de derde aan wie wordt verstrekt, kan de betrokkene bij de beheerder te allen tijde bezwaar aantekenen tegen die verwerking in verband met zijn bijzondere persoonlijke omstandigheden.
2. Binnen vier weken na ontvangst van het bezwaar beoordeelt de beheerder of dit verzet gerechtvaardigd si.
3. De beheerder beëindigt de verwerking terstond, indien hij het verzet gerechtvaardigd acht.
4. Verzet tegen de verwerking met het oog op werving voor commerciële of charitatieve doelen (direct marketing) is altijd gerechtvaardigd.

Artikel 18 Rechtsbescherming

1. Tegen een ontvangen afwijzing op een verzoek tot inwilliging van de bovengenoemde rechten kan de betrokken zich wenden tot de rechtbank van het arrondissement waartoe zijn woonplaats behoort, met het schriftelijk verzoek de beheerder te bevelen alsnog het verzoek toe te wijzen, dan wel het verzet te honoreren.
2. Het verzoekschrift moet worden ingediend binnen zes weken na ontvangst van het antwoord van de beheerder. Indien de beheerder niet binnen de reactietermijn heeft geantwoord, moet het verzoekschrift worden ingediend binnen zes wegen na afloop van de reactietermijn.
3. De betrokkene kan zich ook binnen zes weken wenden tot de Autoriteit Persoonsgegevens, Postbus 93374, 2509 AJ Den Haag, met het verzoek te bemiddelen of te adviseren in zijn/haar geschil met de verantwoordelijke.
4. Wanneer dit verzoek tot bemiddeling of advisering wordt ingediend, kan een verzoekschrift als bedoeld in lid 1 nog aanhangig gemaakt worden nadat de betrokkenen van de Autoriteit Persoonsgegevens (AP) bericht heeft ontvangen dat de behandeling van de zaak is beëindigd, doch uiterlijk zes weken na dat tijdstip.

Artikel 19 Onvoorzien

In de gevallen waarin dit reglement niet voorziet beslist het bestuur.

Artikel 20 Publicatie reglement

Een afschrift van dit reglement is op het bureau van de stichting SWV Helmond-Peelland VO voorhanden. Op diens verzoek stelt de beheerder een exemplaar van dit reglement beschikbaar aan de betrokkene. Een ieder die daarom verzoekt kan hierin inzage krijgen.

Op de website van stichting SWV Helmond-Peelland VO is dit reglement openbaar gemaakt.

Artikel 21 Wijzigingen

1. Wijzigingen in doel van de verwerking en in soort van inhoud, gebruik en wijze van verkrijging van de persoonsgegevens kunnen leiden tot wijziging of aanvulling van verwerkingen zoals vermeld in de bijlagen.
2. Wijziging en aanvulling van dit reglement wordt vastgesteld door het bestuur.

Artikel 22 Citeertitel

Dit reglement kan worden aangehaald als het “Privacyreglement SWV Helmond-Peelland VO.” Dit privacyreglement is vastgesteld door het algemeen bestuur op 23 januari 2017.

BIJLAGE 1
Algemene toelichting op het verwerken van persoonsgegevens

Onder het verwerken van persoonsgegevens verstaat de Wbp elke handeling of elk geheel van handelingen met betrekking tot die persoonsgegevens. Het is dus een zeer ruim begrip. De Wbp noemt een aantal handelingen die als verwerking worden aangeduid: het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

Een verwerking kan uit een of meer van deze handelingen bestaan. Verwerkingshandelingen die in het maatschappelijk verkeer als een eenheid worden beschouwd, worden gezien als één gegevensverwerking. Zo wordt bijvoorbeeld een cliëntadministratie of een klachtenregistratie als één gegevensverwerking beschouwd.

Doel van het melden aan de Autoriteit Persoonsgegevens (AP)
Meldingen van gegevensverwerkingen zorgen voor openheid en daarmee controleerbaarheid voor de betrokkenen. Dat zijn personen van wie verantwoordelijken gegevens gebruiken. De meldingen stellen betrokkenen in staat om zo nodig gebruik te maken van hun rechten.

Melden of niet-melden van een gegevensverwerking
De geheel of gedeeltelijk geautomatiseerde gegevensverwerking dient te worden gemeld bij de Autoriteit persoonsgegevens (AP). Een handmatige gegevensverwerking hoeft in beginsel niet te worden gemeld. Dit is alleen anders indien de handmatige gegevensverwerking is onderworpen aan een voorafgaand onderzoek. Het gaat daarbij om verwerkingen die naar het oordeel van de wetgever een bijzonder risico inhouden voor de persoonlijke levenssfeer van betrokkenen.

Geen meldingsplicht
De verplichting een gegevensverwerking te melden is niet van toepassing op openbare registers die bij wet zijn ingesteld, zoals het handelsregister van de Kamer van Koophandel en het Kadaster. Ook voor verstrekkingen van persoonsgegevens aan een bestuursorgaan wegens een wettelijke verplichting bestaat geen meldingsplicht. Van de meldingsplicht zijn ook vrijgesteld de verwerkingen die in het Vrijstellingsbesluit Wbp staan beschreven.

Vrijstellingsbesluit Wbp
De verwerkingen die staan beschreven in het Vrijstellingsbesluit Wbp zijn vrijgesteld van de meldingsplicht. De vrijstellingen hebben betrekking op verwerkingen die veel voorkomen, die standaard zijn, die met waarborgen omkleed zijn en waarvan algemeen bekend is dat deze plaatsvinden. Zo zullen leden van een sportvereniging in het algemeen ervan op de hoogte zijn dat hun gegevens vastgelegd worden in een ledenadministratie, die de vereniging gebruikt voor het innen van contributie, het organiseren van verenigingsactiviteiten en het verzenden van een clubblad.

Beoordelen gegevensbewerking
Verwerkingen zijn niet van melding vrijgesteld als:
- er meer dan één verantwoordelijke is;
- er gegevens naar landen buiten de Europese Unie worden doorgegeven, tenzij aan bijzondere voorwaarden is voldaan (zie hiervoor de Handreiking Vrijstellingsbesluit);
- een gegevensverwerking specifieke risico's kent en daarom een voorafgaand onderzoek nodig is.

BIJLAGE 2
Gegevensverwerking en vrijstellingen binnen SWV Helmond-Peelland VO

Op grond van de Wbp dient de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens in beginsel te worden gemeld. De verwerkingen die worden beschreven in het Vrijstellingsbesluit Wbp zijn echter van deze wettelijk meldingsplicht uitgesloten (zie voor een toelichting bijlage 1).
Hieronder is een lijst opgenomen met verwerkingen binnen het SWV Helmond-Peelland VO die van de meldingsplicht zijn uitgezonderd. Tevens zijn de relevante artikelen uit het Vrijstellingsbesluit Wbp opgenomen. In deze artikelen is terug te vinden:

1. het doel waarvoor de gegevens mogen worden verwerkt;
2. van wie de persoonsgegevens mogen worden verwerkt (de betrokkenen);
3. welke gegevens mogen worden verwerkt;
4. aan wie gegevens mogen worden verstrekt (ontvangers);
5. bewaartermijnen van de gegevens.

Alleen als aan de vereisten uit de wet is voldaan, is de vrijstelling van toepassing.

Vrijgestelde verwerkingen binnen SWV Helmond-Peelland VO

Bestuur Stichting SWV Helmond-Peelland VO
- bestuursadministratie (art. 3 Vrijstellingsbesluit Wbp)
- oud-personeelsleden (art. 41 Vrijstellingsbesluit Wbp)

Arbeid en pensioen
- Sollicitanten (art. 5 Vrijstellingsbesluit Wbp)
- Personeelsadministratie (art. 7 Vrijstellingsbesluit Wbp)
- Personeelsinformatiesysteem (art. 7 Vrijstellingsbesluit Wbp)
- Salarisadministratie (art. 8 Vrijstellingsbesluit Wbp)
- Uitkering bij ontslag (art.9 Vrijstellingsbesluit Wbp)
- Pensioen of vervroegde uittreding (art. 10 Vrijstellingsbesluit Wbp)

Goederen en diensten
- Debiteuren en crediteuren (art. 12 Vrijstellingsbesluit Wbp)
- Financiële administratie (art. 12 Vrijstellingsbesluit Wbp)
- Afnemers en leveranciers van goederen en diensten en cliënten- en gastenadministratie (art. 13 Vrijstellingsbesluit Wbp)
- Zaken in het kader van huur en verhuur van roerende en onroerende zaken (art. 14 Vrijstellingsbesluit Wbp)

Onderwijs/school
- Leerlingen, docenten of begeleiders (art. 19 Vrijstellingsbesluit Wbp)
- Personeelsgegevens (art. 7 Vrijstellingsbesluit Wbp)
- Oud-personeelsleden (artikel 41 Vrijstellingsbesluit Wbp)

Archieven
- Archiefbeheer (art. 29 Vrijstellingsbesluit Wbp)

Beheer en beveiliging
- Documentenbeheer (art. 31 Vrijstellingsbesluit Wbp)
- Postverwerking (art. 31 Vrijstellingsbesluit Wbp)
- Internet (www.swv-peelland.nl, www.swv-is.nl, aanmeldsite) (art. 32 Vrijstellingsbesluit Wbp)
- Overige netwerksystemen (art. 32 Vrijstellingsbesluit Wbp)
- Netwerkbeheer (art. 32 Vrijstellingsbesluit Wbp)
- Computersystemen (art. 33 Vrijstellingsbesluit Wbp)
- Computerbeheer (art. 33 Vrijstellingsbesluit Wbp)
- Communicatieapparatuur (incl. telefoon/e-mailverkeer) (art. 34 Vrijstellingsbesluit Wbp)
- Autorisatiebeheer (art. 35 Vrijstellingsbesluit Wbp)
- Toegangscontrole gebouwen en/of informatiesystemen (art. 34 Vrijstellingsbesluit Wbp)
- Bezoekersregistratie (art. 37 Vrijstellingsbesluit Wbp)

Overig

- Bezwaarschriften (art. 39 Vrijstellingsbesluit Wbp)
- Klachten (art. 39 Vrijstellingsbesluit Wbp)
- Gerechtelijke procedures (art. 39 Vrijstellingsbesluit Wbp)
- Communicatiebestanden (art. 42 Vrijstellingsbesluit Wbp)
- Adressenlijst (art. 42 Vrijstellingsbesluit Wbp)
- Oud-deelnemers (art. 41 Vrijstellingsbesluit Wbp)
- Oud-personeelsleden (art. 41 Vrijstellingsbesluit Wbp)

De integrale tekst van het vrijstellingsbesluit is te raadplegen middels de bijgevoegde link Vrijstellingsbesluit Wbp. Het besluit kan ook worden gevonden op de website van de AP: https://autoriteitpersoonsgegevens.nl/nl. Op de website van de AP is tevens een handreiking terug te vinden aan de hand waarvan snel kan worden vastgesteld of bepaalde gegevens zijn vrijgesteld van de meldingsplicht.

Bewerkersovereenkomst

Ondergetekenden

SWV Helmond-Peelland VO, ingeschreven bij de Kamer van Koophandel onder nummer 17111027, gevestigd en kantoorhoudende aan Berkveld 19 te 5709 AE Helmond, te dezen rechtsgeldig vertegenwoordigd door de directeur [naam], (hierna te noemen: '**verantwoordelijke'**).

En

[Bedrijfsnaam], ingeschreven bij de Kamer van Koophandel onder nummer [nummer] gevestigd en kantoorhoudende aan [adres], te dezen rechtsgeldig vertegenwoordigd door de directeur, [naam] (hierna te noemen: **'bewerker'**)

Overwegende dat

A. Verantwoordelijke en Bewerker een overeenkomst hebben gesloten (hierna: **'Onderliggende Overeenkomst'**) met betrekking tot het uitvoeren van bepaalde werkzaamheden c.q. het leveren van bepaalde diensten door Bewerker, zoals beschreven in artikel 1.1. van deze Bewerkingsovereenkomst;
B. In het kader van de uitvoering van de Onderliggende Overeenkomst persoonsgegevens worden verwerkt door Bewerker, welke door Verantwoordelijke aan Bewerker worden verstrekt;
C. De hiervoor genoemde gegevens worden aangemerkt als persoonsgegevens, (hierna: **'Persoonsgegevens'**) in de zin van de Wet Bescherming persoonsgegevens (hierna: **'Whp'**);
D. D. Partijen hun afspraken over het verwerken van de Persoonsgegevens schriftelijk vast te leggen in deze overeenkomst in de zin van artikel 14 Wbp (hierna: **'Bewerkersovereenkomst'**).

Zijn het volgende overeengekomen:

Artikel 1. Strekking overeenkomst, doeleinden verwerking
1.1
Bewerker verbindt zich onder voorwaarden van deze Bewerkersovereenkomst in opdracht van Verantwoordelijke Persoonsgegevens te verwerken. Verwerking zal uitsluitend plaatsvinden in het kader van uitvoering van de Onderliggende Overeenkomst, hetgeen het doel is van de verwerking door Bewerker, welke ziet op de volgende werkzaamheden/diensten: […..].
1.2
De Persoonsgegevens die Verantwoordelijke aan Bewerker verstrekt en Bewerker verwerkt zijn opgesomd in bijlage 1.
1.3
De in opdracht van Verantwoordelijke te verwerken persoonsgegevens blijven eigendom van Verantwoordelijke en/of de Betrokkenen.
1.4
Bewerker zal de persoonsgegevens exclusief voor Verantwoordelijke en niet voor enig ander doeleinde verwerken dan zoals in artikel 1.1. is beschreven. Verantwoordelijke zal Bewerker op de hoogte stellen van de doeleinden voor zover deze niet reeds in deze Bewerkersovereenkomst zijn genoemd.

Artikel 2. Totstandkoming, duur en beëindiging overeenkomst
2.1
Deze Bewerkersovereenkomst treedt in werking door ondertekening door Partijen en is van kracht gedurende de looptijd van de Onderliggende Overeenkomst. Indien de Onderliggende Overeenkomst eindigt, eindigt automatisch deze Bewerkersovereenkomst.[1]

[1] Het verdient aanbeveling om in het onderliggende contract op te nemen dat: bij niet-nakoming van de bewerkersovereenkomst de onderliggende overeenkomst kan worden opgezegd zonder dat de Verantwoordelijke op enigerlei schadeplichtig is.

2.2.
Geen van beide Partijen kan deze Bewerkersovereenkomst tussentijds opzeggen.

2.3
Zodra de Bewerkersovereenkomst eindigt dient de Bewerker alle Persoonsgegevens die bij haar aanwezig zijn en eventuele kopieën daarvan te retourneren en te vernietigen. Bewerker zal dan Verantwoordelijke een certificaat/schriftelijk bewijs verstrekken waarin de vernietiging van de Persoonsgegevens wordt bevestigd.

Artikel 3. Verplichtingen Bewerker
3.1
Bewerker zegt toe zorg te dragen voor de naleving van de toepasselijke wet- en regelgeving, waaronder in ieder geval begrepen de Wbp.
3.2
Bewerker zal Verantwoordelijke, op diens verzoek, informeren over de door haar genomen maatregelen aangaande haar verplichtingen onder deze Bewerkersovereenkomst.
3.3
De verplichtingen van de Bewerker die uit deze Bewerkersovereenkomst voortvloeien, gelden ook voor degenen die persoonsgegevens verwerken onder het gezag van Bewerker, waaronder begrepen maar niet beperkt tot werknemers in de ruimste zin van het woord.
3.4
De toegestane verwerkingen zullen te allen tijde worden uitgevoerd binnen een geautomatiseerde/digitale omgeving.
3.5
Bewerker dient Verantwoordelijke onmiddellijk te informeren over enige nalatigheid in de nakoming van de bepalingen uit deze Bewerkersovereenkomst.

Artikel 4. Beveiliging
4.1
Bewerker neemt passende technische en organisatorische maatregelen teneinde de Persoonsgegevens te beveiligen tegen verlies, openbaarmaking, of tegen enige vorm van onrechtmatige verwerking, zoals onbevoegde kennisname, aantasting, wijzigen of verstrekking van de persoonsgegevens.
4.2
Bewerker treft in ieder geval de volgende maatregelen:

a. encryptie (versleuteling) van digitale bestanden met Persoonsgegevens;
b. beveiliging van netwerkverbindingen via Secure Socket Layer (SSL) technologie;
c. passende autorisaties in de omgeving waarin de Persoonsgegevens worden verwerkt.

4.3
Indien een van de maatregelen zoals omschreven in lid 2 van dit artikel ontbreekt, zal Bewerker Verantwoordelijke hierover gemotiveerd informeren en zich inspannen om een passend alternatief van beveiliging te kiezen – eventueel in overleg met Verantwoordelijke, dat gelet op de stand van de techniek, de aard van de Persoonsgegevens en de aan het treffen van de beveiliging verbonden kosten, passend en redelijk is.
Bewerker laat jaarlijks een audit uitvoeren door een externe partij en stelt Verantwoordelijke op de hoogte van het resultaat van deze audit, dan wel verstrekt Verantwoordelijke op verzoek een afschrift van een certificaat van de audit.

Artikel 5. Doorgifte van persoonsgegevens, inschakelen subbewerkers
5.1
Bewerker mag de Persoonsgegevens die zij ontvangt van Verantwoordelijke, niet zonder toestemming van Verantwoordelijke verstrekken of ter beschikking stellen aan derden.
5.2
Bewerker mag de persoonsgegevens slechts verwerken in landen binnen de Europese Economische Ruimte. Doorgifte naar, opslag in of verwerking in landen buiten de Europese Economische Ruimte is verboden.

5.3
Bewerker schakelt geen derden in (zoals subbewerkers) in zonder voorafgaande toestemming van Verantwoordelijke. Verantwoordelijke kan aan de toestemming om derden in te schakelen voorwaarden verbinden.
5.4
Bewerker informeert Verantwoordelijke over de locaties/landen waarin zij Persoonsgegevens verstrekt, waaronder in ieder geval de locatie van het datacentrum/servers wordt verstaan.

Artikel 6. Meldplicht datalekken
6.1
Bewerker zal iedere inbreuk op de beveiliging c.q. datalek als bedoeld in de zin van de Wbp binnen 12 uur nadat het lek is ontdekt melden aan de Verantwoordelijke (M.Q. van Leeuwen, directeur SWV Helmond-Peelland VO[2]), ongeacht of deze inbreuk/datelek aan de Autoriteit Persoonsgegevens dan wel aan betrokkenen gemeld moet worden. De Verantwoordelijke zal vervolgens beoordelen of de datalek aan de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen moet worden gemeld.
6.2.
De melding van Bewerker aan Verantwoordelijke omhelst in ieder geval het melden van het feit dat er een inbreuk op de beveiliging c.q. datalek is geweest, alsmede:

a. wat de (vermeende) oorzaak is van het lek;
b. aard en omvang van het lek;
c. wat het (vooralsnog bekende en/of te verwachten) gevolg is;
d. wat de (voorgestelde) oplossing is.

Bewerker doet de melding aan Verantwoordelijke op basis van de informatie die op dat moment bij hem bekend is. De melding kan later worden aangevuld.
6.3
Bewerker zal Verantwoordelijke op diens verzoek van alle nodige informatie voorzien die Verantwoordelijke nodig heeft om aan de meldplicht als bedoeld in art. 34a Wbp te kunnen voldoen.

Artikel 7. Geheimhouding en vertrouwelijkheid
7.1
Bewerker en diens personeel, dan wel personen die in opdracht van Bewerker werkzaamheden uitvoeren, dienen de aangeleverde Persoonsgegevens strikt vertrouwelijk te behandelen.
7.2
De geheimhoudingsplicht als bedoeld in lid 1 van dit artikel, is niet van toepassing voor zover Verantwoordelijke uitdrukkelijke toestemming heeft gegeven om de informatie aan derden te verschaffen, indien het verstrekken van de informatie aan derden logischerwijs noodzakelijk is gezien de aard van de verstrekte opdracht en de uitvoering van deze Bewerkersovereenkomst, of indien er een wettelijk verplichting bestaat om de informatie aan een derde te verstrekken.

Artikel 8. Verzoek Betrokkene tot inzage, wijziging of verwijdering van gegevens
8.1
Verantwoordelijke draagt zorg voor het afhandelen van verzoeken van Betrokkenen tot inzage van alle verwerkingen zoals bedoeld in artikel 35 Wbp, of verbetering, aanvulling, wijziging, verwijdering of afscherming zoals bedoel in artikel 36 Wbp.
8.2
Bewerker dient medewerking te verlenen aan Verantwoordelijke om te kunnen voldoen aan haar verplichting uit artikel 8.1. en zal op dienst verzoek alle nodige informatie aan Verantwoordelijke verstrekken.
8.3

[2] *Bereikbaar op de volgende manier:*
- *E-mail (m.vanleeuwen@swv-peelland.nl) met ontvangst- en leesbevestiging,*
- *Vaste telefoon (0492-792700)*
- *Mobiele telefoon (06-55152030)*

Bewerker blijft contact met het contactpersoon zoeken totdat Bewerker de leesbevestiging van de e-mail heeft ontvangen dan wel tot Bewerker de contactpersoon heeft gesproken

In het geval dat een betrokkene zich wendt tot Bewerker met een verzoek tot inzage, zoals bedoeld in artikel 35 Wbp, of verbetering, aanvulling, wijziging, verwijdering of afscherming, zoals bedoel in artikel 36 Wbp, zal Bewerker zich inspannen het verzoek zelf af te handelen. Bewerker stelt Verantwoordelijke van de afhandeling van het verzoek op de hoogte. Indien Bewerker niet in staat is het verzoek van Betrokkene af te handelen, stelt zij Verantwoordelijke hiervan op de hoogte en draagt het verzoek van de Betrokkene over aan Verantwoordelijke.

Artikel 9. Aansprakelijkheid
9.1
Bewerker is aansprakelijk voor alle schade voortvloeiende uit of verband houdend met het niet nakomen van deze Bewerkersovereenkomst, dan wel handelen in strijd met de Wbp.
9.2
Bewerker vrijwaart Verantwoordelijke tegen aanspraken van derden, waaronder betrokkenen, alsmede voor boetes van toezichthouders als gevolg van een handeling verricht door Bewerker, in verband met het toerekenbaar tekortschieten van Bewerker in de nakoming van de Bewerkersovereenkomst of overtreding van Wbp en zal daarmee verband houdende en daaruit voortvloeiende kosten (waaronder begrepen kosten van juridische bijstand) en schade aan Verantwoordelijke vergoeden.

9.3
Tenzij nakoming door Bewerker blijvend onmogelijk is, ontstaat de aansprakelijkheid van Bewerker wegens toerekenbare tekortkoming in de nakoming van de Overeenkomst slechts indien Verantwoordelijke de Bewerker schriftelijk in gebreke stelt, waarbij een redelijke termijn voor nakoming dan wel herstel van de tekortkoming, wordt gesteld, en Bewerker ook na die termijn toerekenbaar blijft tekortschieten in de nakoming van haar verplichtingen.

Artikel 10. Slotbepalingen
10.1
Deze Bewerkersovereenkomst en de uitvoering daarvan worden beheerst door Nederlands recht.
10.2
Alle geschillen, welke tussen Partijen mochten ontstaan in verband met de Bewerkersovereenkomst, zullen worden voorgelegd aan de bevoegde rechter voor het arrondissement waarin Verantwoordelijke is gevestigd.
10.3
De inhoud van deze Bewerkersovereenkomst kan enkel schriftelijk worden gewijzigd, met instemming van beide partijen.

Aldus overeengekomen en ondertekend door partijen:

Verantwoordelijk	Bewerker
_____	_____
Naam: [naam]	Naam: [naam]
Functie: Directeur SWV Helmond-Peelland VO	Functie: [functie]
Datum: [datum]	Datum: [datum]

<u>Bijlage bij bewerkingsovereenkomst:</u> Persoonsgegevens die Verantwoordelijke aan Bewerker verstrekt en Bewerker verwerkt
SWV Helmond-Peelland VO registreert persoonsgegevens in het digitale informatiesysteem (DIS) van Bui Engineering van leerlingen uit het samenwerkingsverband. De geregistreerde persoonsgegevens hebben allemaal betrekking op het onderwijskundige aspect en zijn bedoeld om alle activiteiten ten behoeve van het onderwijs uit te kunnen voeren.

De geregistreerde persoonsgegevens omvatten:

- *Naam*
- *Adresgegevens*
- *Geboortedatum*
- *Bsn*
- *E-mailadres ouder(s)/verzorger(s)*

BIJLAGE 4

Zorgvuldigheidsverklaring persoonsgegevens

1. In het algemeen doe ik niets wat ongeoorloofde inbreuk op de persoonsgegeven betreft.
2. In ga zorgvuldig om met het delen van persoonsgegevens zoals e-mailadressen en persoonlijke telefoonnummers.
3. Ik laat wachtwoorden en/of persoonlijke toegangscodes en/of sleutels die aan mij verstrekt zijn in het kader van mijn werkzaamheden voor het SWV Helmond-Peelland VO niet onbeheerd achter: ze zijn niet zichtbaar en/of toegankelijk en/of beschikbaar voor derden.
4. Wachtwoorden en toegangscodes zijn persoonlijk. Ik verstrek die niet aan derden. Tot het tegendeel bewezen is, ben ik persoonlijk verantwoordelijk voor de gevolgen, als een derde met behulp van mijn persoonlijke wachtwoord, zich toegang heeft verstrekt tot privacygevoelige gegevens.
5. Als ik mijn werkplek verlaat, vergrendel ik het beeldscherm van mijn computer ( + L gelijktijdig indrukken).
6. Als ik afdrukken maak, gebruik ik altijd de aan mij verstrekte persoonlijke code.
7. Als ik afdrukken van documenten waarin privacygevoelige gegevens zijn opgenomen, laat ik de printer niet onbeheerd achter tijdens het afdrukken van die documenten.
8. Ik heb standaard uitsluitend toegang tot persoonsgegevens in het kader van mijn werkzaamheden voor het SWV Helmond-Peelland VO, via vaste personal computers.
9. Ik zorg ervoor dat de persoonsgegevens waarover ik in het kader van mijn werkzaamheden voor SWV Helmond-Peelland VO kan beschikken, niet onbeveiligd opgeslagen worden op portable devices zoals laptop, telefoon, usb-sticks, etc.);
10. Als ik van mening ben dat het noodzakelijk is om persoonsgegeven op een draagbaar medium te plaatsen, doe ik dat uitsluitend op usb-sticks die beveiligd zijn met een wachtwoord en die door de office manager (en bij diens afwezigheid de directeur) beheerd worden en waarvan de office manager een administratie bijhoudt.
11. De genummerde, met wachtwoord beveiligde usb-sticks, die uitsluitend door werknemer worden gebruik voor werkzaamheden voor het SWV Helmond-Peelland VO, maak ik na gebruik leeg en lever ik in bij de office manager van SWV Helmond-Peelland VO.
12. De kantoren van SWV Helmond-Peelland VO zijn uitsluitend toegankelijk voor medewerkers van het SWV Helmond-Peelland VO.
13. Indien derden verblijven in de kantoren van het SWV Helmond-Peelland, is dat in aanwezigheid van en onder verantwoordelijkheid van een medewerker.
14. Derden die een afspraak hebben met een medewerker van het SWV Helmond-Peelland VO gebruiken niet de kantoorruimten van SWV Helmond-Peelland VO als wachtruimte.
15. Ik ga zorgvuldig om met e-mailadressen door, bij groepsmail, indien mogelijk gebruik te maken van ‘bcc’ in plaats van ‘aan’ of ‘cc’.
16. Ik verstrek niet zonder meer e-mailadressen aan derden.
17. Ik neem in mijn e-mails een disclaimer op namelijk: *De inhoud van dit bericht is alleen bestemd voor de geadresseerde en kan vertrouwelijke of persoonlijke informatie bevatten. Als u dit bericht onbedoeld heeft ontvangen verzoeken wij u het te vernietigen en de afzender te informeren. Het is niet toegestaan om een bericht dat niet voor u bestemd is te vermenigvuldigen dan wel te verspreiden.*
18. Persoonsgegevens van leerlingen worden bij voorkeur via de beveiligde internetomgeving van het digitaal informatiesysteem (DIS) van het SWV Helmond-Peelland VO uitgewisseld.
19. Als er telefonisch persoonsgegevens opgevraagd worden, en ik de identiteit van de beller niet kan vaststellen, dan beëindig ik het gesprek en neem zelf telefonisch contact op via het vaste nummer van de organisatie namens wie de beller zegt contact op te nemen om te verifiëren of beller inderdaad namens betreffende organisatie belt.

20. Als ik op een van de hierboven genoemde punten niet heb gehandeld volgens afspraak, meld ik dat aan directeur.
21. Als ik van mening ben dat er privacygevoelige informatie is gelekt binnen de eigen of een organisatie met wie beroepsmatig word samengewerkt, meld ik dat zo snel mogelijk maar in ieder geval binnen 24 uur bij de directeur en indien deze onbereikbaar is, bij de voorzitter van SWV Helmond-Peelland VO

Naam medewerker	Functie	Datum	Handtekening

Protocol datalekken

Inleiding
Iedereen heeft recht op eerbiediging en bescherming van zijn persoonlijke levenssfeer en een zorgvuldige omgang met zijn persoonsgegevens. De regels hieromtrent zijn vastgelegd in de Wet bescherming persoonsgegevens (Wbp).
Persoonsgegevens die worden verwerkt dienen te zijn beveiligd tegen verlies en onrechtmatige verwerking. Sinds 1 januari 2016 geldt de meldplicht datalekken. Er is sprake van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens[3]. De persoonsgegevens zijn dan blootgesteld aan verlies of onrechtmatige verwerking[4]. Een datalek moet gemeld worden bij de Autoriteit Persoonsgegevens als het leidt tot (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens. Een melding van het datalek aan de betrokkene kan nodig zijn als het waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer[5]. In deze notitie is een schets[6] van het juridische kader opgenomen. Om te kunnen bepalen of er daadwerkelijk sprake is van een datalek wat moet worden gemeld bij de Autoriteit Persoonsgegevens is een protocol opgesteld. In dit protocol is het juridisch kader verwerkt. Eveneens bevat het een procedurebeschrijving voor de melding van het datalek aan de functionaris gegevensbescherming, aan de Autoriteit Persoonsgegevens en indien nodig aan de betrokkene(n).

Juridisch kader
Persoonsgegevens
De meldplicht datalekken is enkel van toepassing als er sprake is van de verwerking van persoonsgegevens. Een persoonsgegeven is (op grond van artikel 1 sub a Wbp) elk gegeven betreffende een geïdentificeerde of identificeerbare persoon. Hiervan is sprake indien de identiteit redelijkerwijs, dus zonder onevenredige inspanning, vastgesteld kan worden. Het maakt niet uit of de identiteit van de persoon zonder veel omwegen eenvoudig is vast te stellen[7] of dat de gegevens via nadere stappen in verband kunnen worden gebracht met een bepaalde persoon[8]. De verwerking van persoonsgegevens betreft – zoals bepaald in artikel 1 sub b Wbp – elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens. Hieronder valt in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Verantwoordelijke
De meldplicht datalekken richt zich enkel tot de verantwoordelijke voor de verwerking van persoonsgegevens. Met de verantwoordelijke wordt hier degene bedoeld die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.[9] Het gaat hierbij om de vraag wie bepaalt op welke manier de gegevensverwerking zal plaatsvinden.

Bewerker
Veel verantwoordelijken laten de verwerking van hun persoonsgegevens geheel of gedeeltelijk uitvoeren door een zogeheten bewerker. De bewerker verwerkt persoonsgegevens ten behoeve van de verantwoordelijke zonder dat diegene aan het rechtstreekse gezag van de verantwoordelijke is onderworpen. Om goede afspraken te maken met de bewerker dient een goede bewerkersovereenkomst te worden gesloten waarbij eveneens afspraken worden gemaakt over de meldplicht datalekken. De bewerkersovereenkomst wordt verder buiten beschouwing gelaten in dit juridisch kader.

[3] Zie artikel 13 Wbp
[4] Hierbij kan worden gedacht aan een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker.
[5] Zie hierover artikel 34a Wbp
[6] Zie voor een zeer uitvoerige behandeling over de meldplicht datalekken: Autoriteit Persoonsgegevens, *beleidsregels meldplicht datalekken,* 9 december 2015
[7] In dat geval is er sprake van direct identificeerbare gegevens
[8] Dan spreken we van indirect identificerende gegevens. Zie verder over de identificeerbaarheid van persoonsgegevens: Autoriteit persoonsgegevens, *beleidsregels meldplicht datalekken,* 9 december 2015
[9] Artikel 1 sub d Wbp

Datalek
De wet spreekt over een datalek als er 'een inbreuk op de beveiliging als bedoeld in artikel 13' heeft voorgedaan. Er is dus alleen sprake van een datalek als er daadwerkelijk een beveiligingsincident heeft voorgedaan, zoals het kwijtraken van een USB-stick, diefstal van een laptop of inbraak door een hacker. Echter, niet ieder beveiligingsincident is een datalek. Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan of als een onrechtmatige verwerking van de betreffende persoonsgegevens niet redelijkerwijs kan worden uitgesloten.

Artikel 13 behelst de verplichting om als verantwoordelijke passende technische en organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Kenmerkend voor de inbreuk op de beveiliging is dat het beveiligingsincident daadwerkelijk gevolgen heeft voor de persoonsgegevens die worden verwerkt. Kortom, er zijn persoonsgegevens verloren gegaan of het is niet redelijkerwijs uit te sluiten dat er persoonsgegevens onrechtmatig zijn verwerkt[10].
Er wordt gesproken over het verlies van persoonsgegevens als de persoonsgegevens niet meer beschikbaar zijn. Dit kan komen doordat de persoonsgegevens zijn vernietigd en er geen complete en actuele reservekopie van de gegevens zijn. In dat geval is er sprake van een datalek.
Ook bij een onrechtmatige verwerking wordt gesproken over een datalek indien het gaat om aantasting van persoonsgegevens, onbevoegde kennisneming, wijziging of verstrekking daarvan.[11]

Melding
Autoriteit Persoonsgegevens
Er is sprake van een geclausuleerde meldplicht voor datalekken. Dat wil zeggen dat volgens de wet enkel een melding hoeft te worden gedaan als het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Om te bepalen of die kans bestaat wordt gekeken naar de aard en omvang van de persoonsgegevens waar het om gaat.
Bij persoonsgegevens van gevoelige aard is een melding noodzakelijk.
Persoonsgegevens van gevoelige aard zijn in ieder geval:

- Gegevens die gaan over godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag;
- Gegevens over iemands financiële of economische situatie;
- Gebruikersnamen, wachtwoorden en andere inloggegevens;
- Gegevens die kunnen worden misbruikt voor (identiteits-)fraude; en
- Gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene.

Ook de hoeveelheid gelekte persoonsgegevens of het aantal betrokkenen van wie er persoonsgegevens zijn gelekt, kunnen betekenen dat het datalek gemeld moet worden. Aldus kunnen aard en omvang van het datalek er toe leiden dat er sprake is van een aanzienlijke kans op ernstige nadelige gevolgen. In de parlementaire geschiedenis en het beleidsdocument van de Autoriteit Persoonsgegevens wordt ook aandacht gevraagd voor kwetsbare groepen, zoals kinderen. Bij het verwerken van persoonsgegevens van minderjarige kinderen moet er van uitgegaan worden dat bij een datalek altijd een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens aanwezig kan zijn. [12]
Als er sprake is van een datalek dan dient zo snel mogelijk een melding bij de functionaris gegevensbescherming te worden gedaan. Hij zal in ieder geval binnen de wettelijke termijn van 72 uur een melding doen bij de Autoriteit Persoonsgegevens.

[10] Een inbreuk moet ruim worden gelegd. Het enkel nemen van maatregelen is niet voldoende. Zie hierover Kamerstukken || 2013/14, 33662 nr. 6, blz. 4
[11] Hierbij valt te denken aan een malware besmetting. Zie voor meer voorbeelden, Autoriteit Persoonsgegevens, *beleidsregels meldplicht datalekken,* p.21 *ev.*
[12] Zie hierover uitgebreid: Handelingen || 2014/15, nr. 51, item 9 en Autoriteit Persoonsgegevens, *Beleidsregels meldplicht datalekken,* 2015, p.28

Betrokkene
Als een datalek waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer dan geeft de wet aan dat er ook een meldplicht is aan de betrokkene(n). Betrokkenen kunnen namelijk door het verlies, onrechtmatig gebruik of misbruik in hun belangen worden geschaad en zij zullen daar eventueel maatregelen tegen moeten nemen. Zo zal bijvoorbeeld een gelekt wachtwoord moeten worden vervangen. De wet schrijft ook hier voor da de melding onverwijld moet gebeuren.
Een melding hoeft echter niet altijd te gebeuren. Wanneer er passende technische maatregelen vooraf zijn genomen waardoor de persoonsgegevens die het betreft onbegrijpelijk of ontoegankelijk zijn voor onbevoegden, dan kan de melding achterwege blijven. Per geval zal steeds moeten worden bepaald of er voldoende beschermingsmaatregelen zijn genomen waardoor een melding al dan niet moet gemaakt.

Boete
Bij een overtreding van de meldplicht datalekken heeft de Autoriteit Persoonsgegevens sanctie bevoegdheden. Zo kan de Autoriteit Persoonsgegevens een bindende aanwijzing opleggen indien een overtreding niet opzettelijk is gepleegd en er geen sprake is van ernstig verwijtbare nalatigheid. Afhankelijk van de omstandigheden van het geval kan de Autoriteit Persoonsgegevens echter ook een bestuurlijke boete op leggen. De bestuurlijke boete bedraagt ten hoogste het bedrag van de 6e categorie van artikel 23 lid 4 Wetboek van Strafrecht.[13] Per 1 januari 2016 bedraagt de boete maximaal € 820.000,-.
De Autoriteit Persoonsgegevens heeft aangegeven zich terughoudend op te stellen indien een organisatie een eigen functionaris voor de gegevensbescherming heeft.

Overig
De wijze waarop een datalek tot stand is gekomen, kan er toe leiden dat behalve een melding dataleken ook aangifte moet worden gedaan bij de politie. Indien het datalek is veroorzaakt door een hack, dan zal er altijd aangifte moeten worden gedaan aangezien een hack wordt gezien als een inbraak.

Protocol
Het bijgevoegde protocol[14] is bedoeld om vast te stellen of er sprake is van een datalek waarop de Wbp ziet. Tevens bevat het een procedure beschrijving voor het melden van het datalek.

In het protocol wordt men aan de hand van zeven vragen begeleid hoe om te gaan met het voorgevallen incident:

1. Is de meldplicht datalekken van toepassing?
2. Is een gebeurtenis te beschouwen als een datalek?
3. Moet het datalek gemeld worden?
4. Hoe en wanneer moet het datalek worden gemeld?
5. Moet het datalek ook worden gemeld aan de betrokkene?
6. Hoe en wanneer moet het datalek worden gemeld aan de betrokkene?
7. Welke gegevens moeten worden gearchiveerd?

[13] De bedragen in dit artikel worden elke 2 jaar aangepast aan de ontwikkeling van de consumentenprijsindex
[14] Zie bijlage 1

PROTOCOL DATALEKKEN

Begrippenlijst

a. Autoriteit Persoonsgegevens: zelfstandig bestuursorgaan dat bij wet als toezichthouder is aangesteld voor het toezicht op de correcte verwerking van persoonsgegevens, voorheen het College bescherming persoonsgegevens;

b. bestand: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen;

c. betrokkene: degene op wie een persoonsgegeven betrekking heeft;

d. bewerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt;

e. bindende aanwijzing: de zelfstandige last die de Autoriteit wegens een overtreding wordt opgelegd;

f. Datalek: beveiligingsinbreuk zoals bedoeld in artikel 13 Wbp;

g. Functionaris persoonsgegevens: persoon, werkzaam bij SWV Helmond-Peelland VO, die is belast met de controle op de naleving van de bepalingen uit de Wbp en datalekken moet melden bij de Autoriteit Persoonsgegevens;

h. Ontvanger: degene aan wie persoonsgegevens worden verstrekt;

i. Persoonsgegevens: elk gegeven betreffende een geïdentificeerde of identificeerbare persoon, zoals bedoeld in artikel 1 sub a Wbp;

j. Persoonsgegevens van gevoelige aard: persoonsgegevens zoals bedoeld in artikel 16 Wbp;

k. Verantwoordelijke: degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking vaststelt. Het inschakelen van derden maakt hier geen uitzondering op;

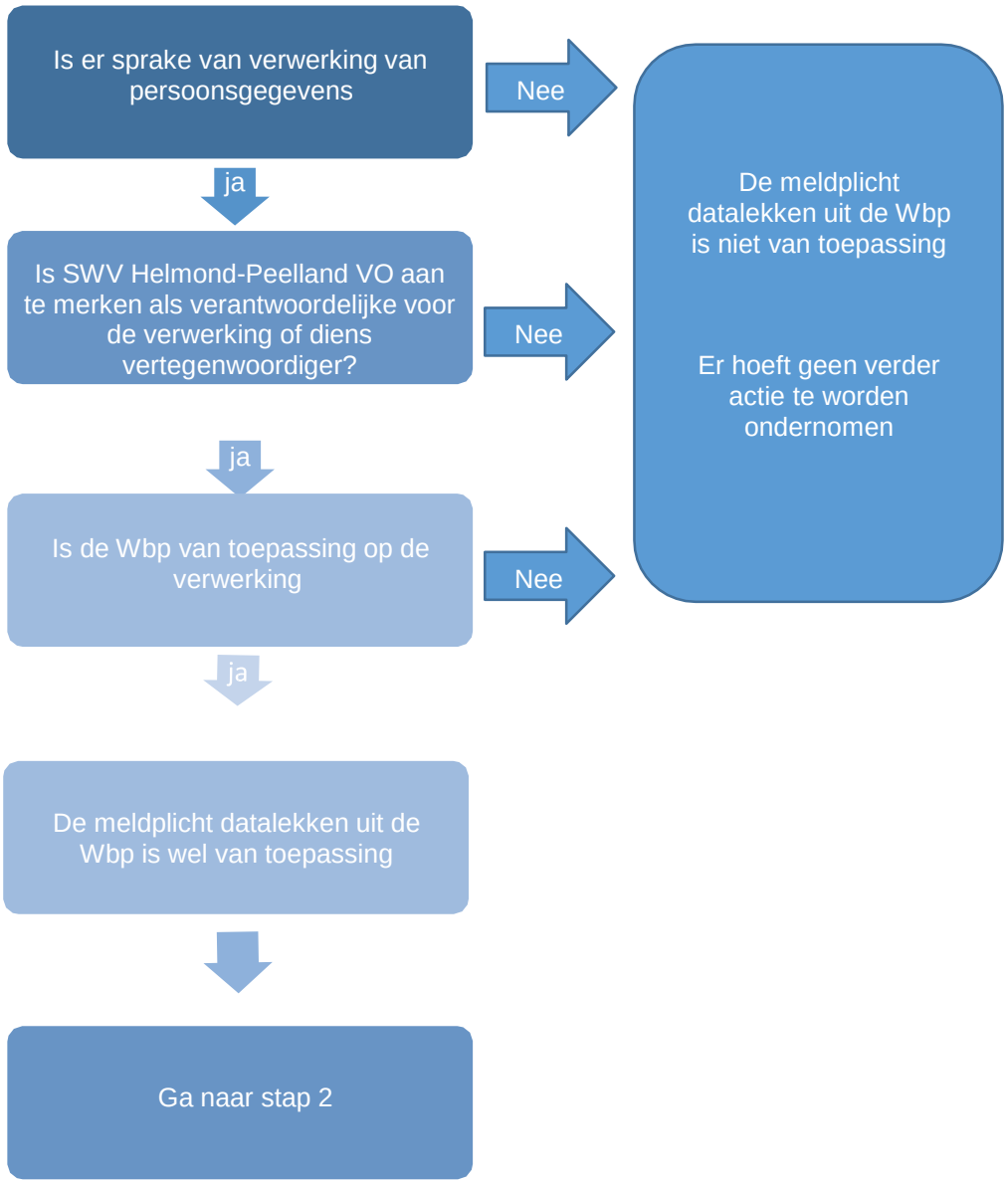
l. Verwerking: verwerking van persoonsgegevens zoals bedoeld in artikel 1 sub b Wbp;

m. Wbp: wet bescherming persoonsgegevens, stb 2015, 230.

1. Is de meldplicht datalekken uit de Wbp van toepassing?

Dat is het geval indien:

a) Er sprake is van verwerking van persoonsgegevens. De verwerking van persoonsgegevens betreft elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, zoals het verzamelen, vastleggen, ordenen, raadplegen en verspreiden.
b) SWV Helmond-Peelland VO is de verantwoordelijke of diens vertegenwoordiger.
c) De Wbp op de verwerking van toepassing is. Bepaalde verwerkingen vallen door hun aard of doelstelling buiten de reikwijdte van de Wbp. In beginsel is op de verwerking van persoonsgegevens binnen SWV Helmond-Peelland VO altijd de Wbp van toepassing.



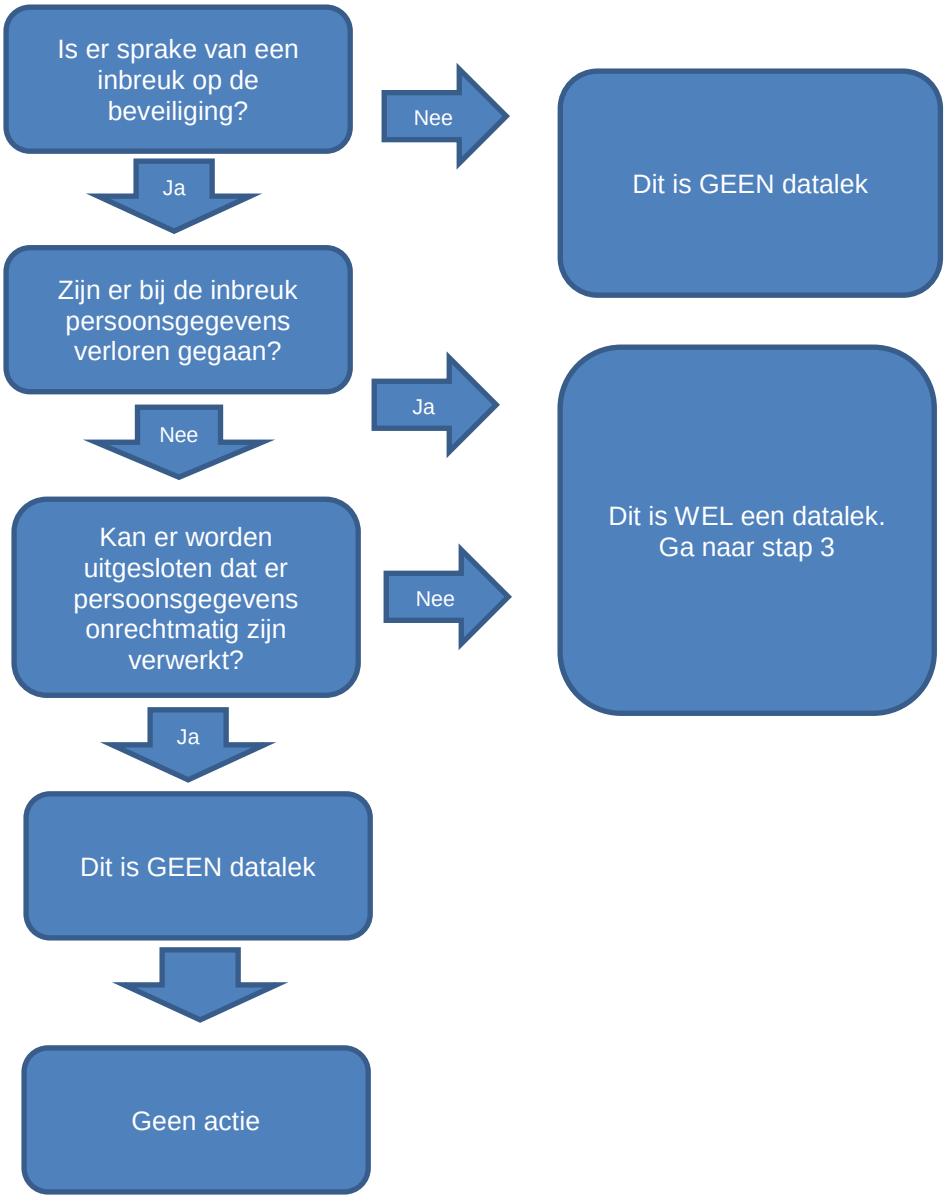
2. Is een gebeurtenis te beschouwen als een datalek?
Als de gebeurtenis valt onder de werking van de Wbp komt men toe aan vraag 2: is er sprake van een datalek?

Dit is het geval indien:

a) Er sprake is van een inbreuk op de beveiliging. Dat wil zeggen dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan

EN

b) Bij de inbreuk persoonsgegevens verloren zijn gegaan of redelijkerwijs niet kan worden uitgesloten dat er persoonsgegevens onrechtmatig zijn verwerkt, waaronder moet worden begrepen de aantasting van de persoonsgegevens, onbevoegde kennisneming, wijziging of verstrekking daarvan.



3. Moet het datalek gemeld worden?

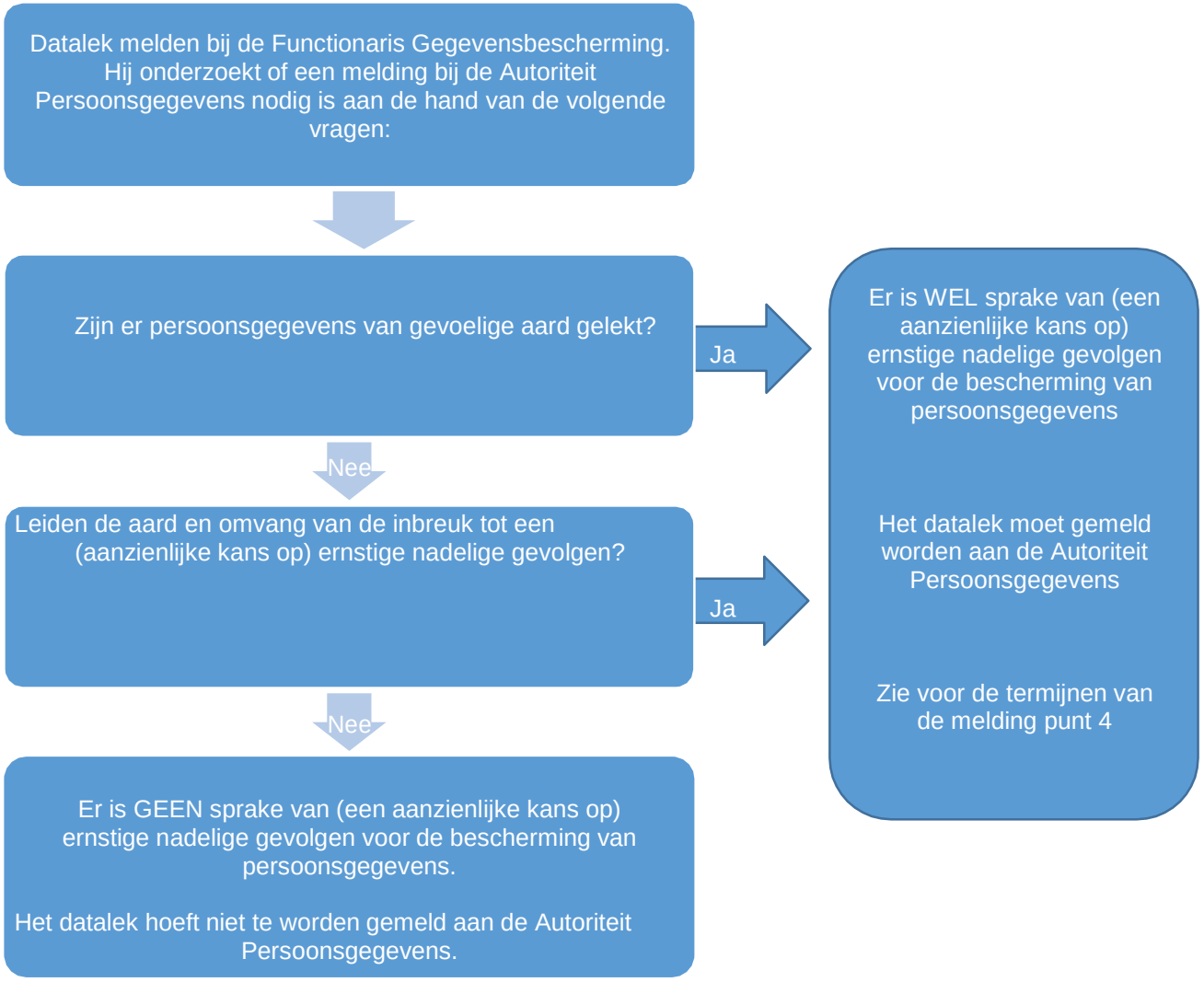
Een datalek moet gemeld worden aan de Functionaris Gegevensbescherming bij SWV Helmond-Peelland VO. Indien sprake is van een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens zal er eveneens een melding worden gedaan aan de Autoriteit Persoonsgegevens. Er is sprake van een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens indien één van de volgende situaties aan de orde is:

A. Persoonsgegevens van gevoelige aard zijn gelekt, namelijk:
   - Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp:
     - Betreffende iemands levensovertuiging of godsdienst, ras, politieke gezindheid, gezondheid, seksuele leven of lidmaatschap van een vakvereniging;
     - Strafrechtelijke persoonsgegevens; en
     - Persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag;

   óf

   - Persoonsgegevens die anderszins van gevoelige aard zijn, waaronder:
     - Gegevens over de financiële of economische situatie van de betrokkene;
     - Gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
     - Gebruikersnamen, wachtwoorden en andere inloggegevens;
     - Gegevens die kunnen worden misbruikt voor (identiteits-)fraude;
     - Gegevens uit DNS-databanken, gegevens waar een bijzondere wettelijke bepaalde geheimhoudingsplicht op rust en gegevens die onder een beroepsgeheim vallen.

B. De aard en omvang van de inbreuk leiden tot (een aanzienlijke kans op) ernstige nadelige gevolgen. Hierbij is van belang:
   - Gaat het om veel persoonsgegevens per persoon of om gegevens van grote groepen?
   - Zijn de beslissingen die op basis van de verwerkte persoonsgegevens worden genomen ingrijpend?
   - Worden de persoonsgegevens binnen ketens gedeeld?
   - Gaat het om persoonsgegevens van kwetsbare groepen?


Datalek melden bij de Functionaris Gegevensbescherming. Hij onderzoekt of een melding bij de Autoriteit Persoonsgegevens nodig is aan de hand van de volgende vragen:
Zijn er persoonsgegevens van gevoelige aard gelekt?
Ja
Nee
Leiden de aard en omvang van de inbreuk tot een (aanzienlijke kans op) ernstige nadelige gevolgen?
Ja
Nee
Er is GEEN sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens.
Het datalek hoeft niet te worden gemeld aan de Autoriteit Persoonsgegevens.
Er is WEL sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens
Het datalek moet gemeld worden aan de Autoriteit Persoonsgegevens
Zie voor de termijnen van de melding punt 4

4. Hoe en wanneer moet het datalek worden gemeld?
Als er het vermoeden is van een datalek moet dit gemeld worden zoals bepaald onder 3. Het is noodzakelijk om de melding te doen binnen de daarvoor geldende termijnen:

Termijn
Een datalek moet onverwijld worden gemeld. Dit houdt in dat de verantwoordelijke na het ontdekken van een mogelijk datalek enige tijd mag nemen voor nader onderzoek. Op deze manier kunnen de voorgaande stappen uit dit protocol kunnen worden doorlopen en kunnen onnodige meldingen worden voorkomen.
De termijn voor het melden begint te lopen op het moment dat de verantwoordelijke of een bewerker op de hoogte raakt van een incident dat mogelijk onder de meldplicht datalekken valt. De melding vindt uiterlijk binnen 72 uur na de ontdekking van het datalek plaats bij de Autoriteit Persoonsgegeven door de Functionaris Persoonsgegevens. Uiteraard alleen als er sprake is van een datalek en het onder de meldplicht datalekken valt.

De melding
Zodra op school een mogelijk datalek is geconstateerd wordt er onverwijld (binnen 12 uur) contact opgenomen met de functionaris gegevens bescherming. De functionaris gegevens bescherming beoordeelt (nogmaals) of er sprake is van een datalek vallend onder de werking van de meldplicht datalekken uit de Wbp. Indien hier sprake van is vindt er een melding plaats bij de Autoriteit Persoonsgegevens.

Aangifte
Indien er sprake is van een datalek kan er vermoeden zijn van strafbaar handelen. Zo is bijvoorbeeld hacken strafbaar gesteld. In die gevallen moet er behalve een melding datalekken bij de functionaris gegevensbescherming, ook aangifte worden gedaan bij de politie.
Een afschrift hiervan moet worden gezonden aan de functionaris gegevensbescherming.

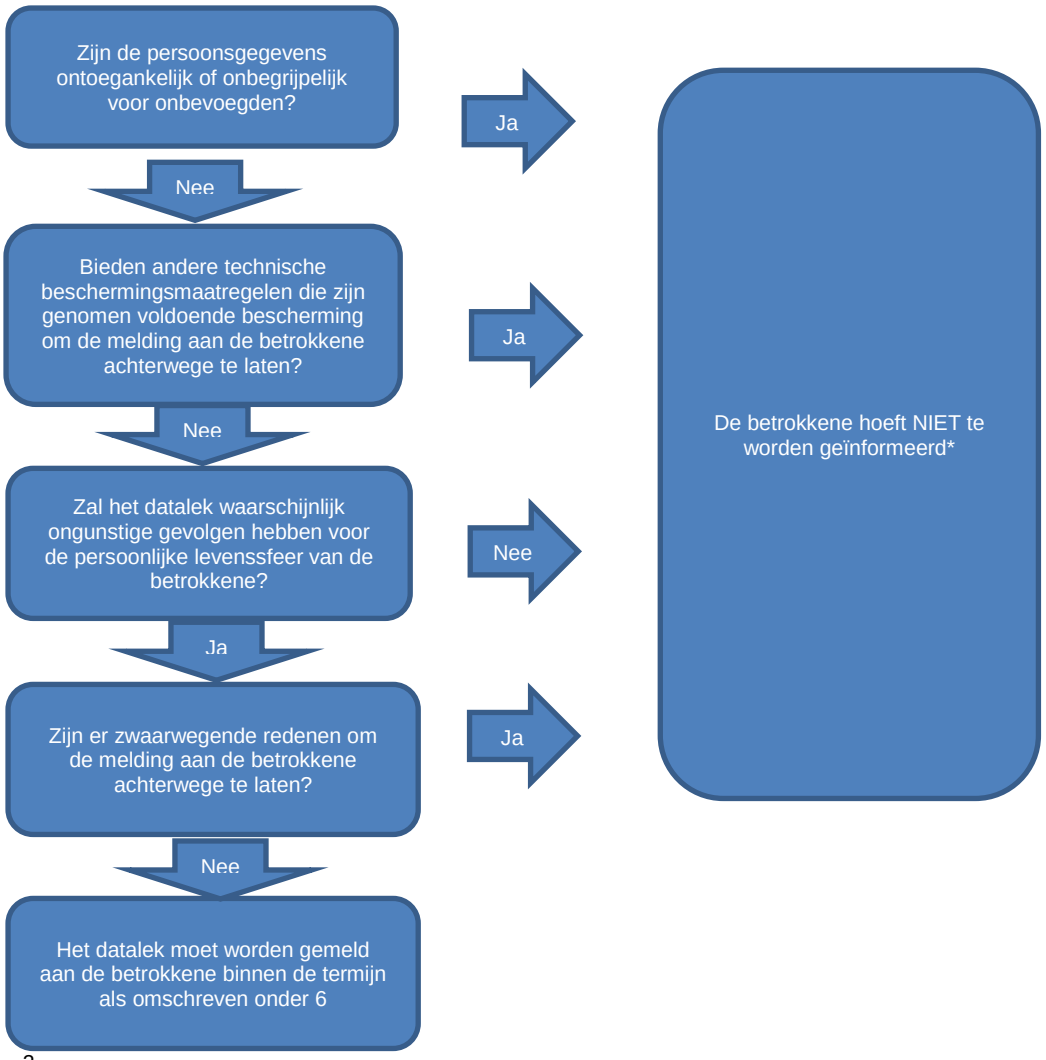
5. Moet het datalek worden gemeld aan degene van wie de persoonsgegevens zijn gelekt?

Het uitgangspunt is dat indien er persoonsgegevens zijn gelekt dat dit wordt gemeld aan degene wiens persoonsgegevens het betreft.

Het datalek hoeft niet te worden gemeld aan de betrokkene indien één van de volgende situaties zich voordoet:

a. Er zijn passende technische beschermingsmaatregelen genomen waardoor de persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens, bijvoorbeeld door adequate encryptie[2] en hashing[3].
b. Andere technische beschermingsmaatregelen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten, bijvoorbeeld door een tijdige en adequate remote wiping[4] en pseudonimisering[5].
c. Het is onwaarschijnlijk dat het datalek ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene. Indien persoonsgegevens van gevoelige aard zijn gelekt, moet het altijd gemeld worden.
d. Er zijn andere zwaarwegende redenen om de melding aan de betrokkene achterwege te laten.

In een stroomschema ziet het er als volgt uit:



[2] Versleuteling

[3] Het omzetten van gegevens in een unieke code

[4] Het op afstand wissen van de gegevens die op een apparaat staan

[5] Technische maatregelen om te voorkomen dat de persoonsgegevens worden gekoppeld aan de oorspronkelijke identiteit van de betrokkene.

*De Autoriteit Persoonsgegevens kan, indien zij van oordeel is dat de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene, verlangen om alsnog een kennisgeving aan betrokkene(n) te doen. Ook al zou dat op basis van het stroomschema niet hoeven.

6. Hoe en wanneer moet de melding worden gedaan aan de betrokkene?

Termijn

Een datalek moet onverwijld worden gemeld. Dat houdt in dat de verantwoordelijke, na het ontdekken van een mogelijk datalek enige tijd mag nemen voor nader onderzoek zodat betrokkene op een behoorlijke en zorgvuldige manier kan worden geïnformeerd.
De betrokkene wordt in ieder geval onmiddellijk geïnformeerd nadat er een melding bij de Autoriteit Persoonsgegevens is gedaan.

Melding

De functionaris gegevensbescherming doet de melding aan de betrokkene (in overleg met de school). In de kennisgeving aan de betrokkene staat in ieder geval het volgende vermeld:

- De aard van de inbreuk;
- De contactgegevens van de functionaris gegevensbescherming; en
- De maatregelen die zijn aanbevolen om de negatieve gevolgen van de inbreuk te beperken.

7. Welke gegevens moeten worden gearchiveerd?

De functionaris gegevensbescherming houdt een overzicht bij van alle datalekken die onder de meldplicht vallen en dus gemeld zijn aan de Autoriteit Persoonsgegevens. Per datalek bevat het overzicht in ieder geval de gegevens omtrent de aard van de inbreuk en, indien aan de betrokkene is gemeld, de tekst van de kennisgeving.

Archivering; Selectielijst

Inleiding
In het kader van de aangescherpte privacywetgeving is het goed archiveren van stukken, maar ook het vernietigen ervan nog belangrijker geworden.
Ten behoeve van een goede archivering schrijft de Archiefwet het gebruik van selectielijsten voor. Tot op dit moment beschikt SWV Helmond-Peelland VO nog niet over een selectielijst. De VO-raad is gestart met het opstellen van een selectielijst voor de sector, maar dit komt vooralsnog niet van de grond. De verwachting is dan ook nu dat er geen selectielijst voor de sector zal komen. Deze notitie bevat een selectielijst voor de eigen organisatie.

Juridisch kader
Artikel 3 van de Archiefwet schrijft voor dat een organisatie haar archiefbescheiden brengt en bewaart in goede, geordende en toegankelijke staat. Onder archiefbescheiden worden alle bescheiden – ongeacht de drager – die door de organisatie zijn ontvangen of opgemaakt en die naar hun aard bestemd zijn daaronder te berusten. Het betreft hier dus niet enkel papieren documenten; Ook digitaal vastgelegde informatie valt onder de werking van de archiefwet.
Het in goede en geordende staat bewaren van de bescheiden houdt onder meer in dat het archief op gezette tijden wordt opgeschoond. In de (verplichte) selectielijst wordt geregeld welke categorieën archiefbescheiden op termijn vernietigd moeten worden en welke voor altijd bewaard blijven. Documenten die onder de Archiefwet vallen mogen namelijk pas worden vernietigd als ze in een geldige selectielijst staan vermeld en daarin als vernietigbaar zijn aangemerkt.

Selectielijst, nog te ontwikkelen
De selectielijst is naar zijn aard een duurzaam instrument. In de selectielijst zijn per organisatieonderdeel de taken en de daarmee samenhangende documenten weergegeven. Deze documenten worden vervolgens voorzien van een (wettelijk) bewaaradvies en/of een toelichting. De opzet van de selectielijst zal zoveel mogelijk aansluiten bij de organisatiestructuur. Ook voor de termijnen van vernietiging is (zo veel als mogelijk) aangesloten bij de huidige praktijk binnen de organisatie.

Vorm
Documenten die volgens de selectielijst permanent bewaard dienen te blijven, moeten in fysieke toestand bewaard blijven. Enkel een digitale versie is dan onvoldoende.