De Uniforme Pensioen Aangifte en databeveiliging

Adviesrapportage over de
risicogebieden en afhandeling van
beveiligingsrisico's met betrekking tot datalekken

<lege pagina>

Inhoud

Werkgroep

Deze adviesrapportage is opgesteld vanuit de werkgroep UPA Databeveiliging. Deze werkgroep is samengesteld uit de volgende leden van de UPA klankbordgroep:

- Pensioenuitvoerders:
  - APG – A. van Leest
  - PGGM – A. Minten
- Softwareontwikkelaars:
  - ADP Nederland B.V. – J. Smits
  - SAP Nederland B.V. – L. Mommersteeg
  - Unit4 Business Software B.V. – J. Sjaardema

Versiebeheer

Versie	Datum	Omschrijving
0.4	13 oktober 2016	Conceptversie werkgroep
0.5	15 december 2016	Conceptversie werkgroep o.b.v. overleg 14 dec.
0.6	30 december 2016	Conceptversie, voorgelegd aan klankbordgroep UPA
0.7	1 februari 2017	Conceptversie werkgroep
1.0	2 februari 2017	Versie voorgelegd aan de high level group
1.1	8 maart 2017	Verwerking van diverse aanbevelingen vanuit de high level group

Doelstelling

Het doel van dit document is om duidelijkheid te creëren en advies te geven over databeveiliging in de vorm van een (proces)beschrijving, die gebruikt wordt bij de uitwisseling van data voor de Uniforme Pensioen Aangifte (UPA). Om deze duidelijkheid te verkrijgen heeft de werkgroep zich gericht op:

- Benoemen van de betrokkenen en hun rollen binnen de UPA-keten;
- Beschrijving van het proces binnen de UPA-keten en de mogelijke beveiligingsrisico's in het kader van een datalek;
- Duidelijkheid verschaffen over databeveiliging;
- Advies over mogelijke vervolgacties, indien er een datalek wordt geconstateerd.

Het document richt zich niet op de technische kant van databeveiliging. Van iedere betrokkene binnen het UPA-proces wordt verwacht dat deze uitsluitend werkt via beveiligde verbindingen om gegevens digitaal uit te wisselen. Iedere betrokken partij wordt geacht een gedegen beleid op IT-security te voeren. Iedere betrokkene heeft een eigen verantwoordelijkheid binnen het proces in het geval van lekken. Deze zijn niet in het document beschreven.

Dit document dient niet alleen door de uitwisselaars van de UPA-data gebruikt te worden, maar dient ook door de Pensioenfederatie bekrachtigd en uitgedragen te worden. Hierdoor wordt dit breder toepasbaar. De klankbordgroep UPA biedt dit document via de high level group aan bij de Pensioenfederatie.

Advies

Afhankelijk van de aard en de positie van het eventuele datalek binnen het proces, wordt geadviseerd om openheid van zaken te geven tussen alle betrokken partijen. Daarbij zal rekening gehouden moeten worden met de gevoeligheid van het onderwerp en de integriteit van alle partijen. Doelstelling van alle betrokkenen moet immers zijn, om schade bij de individuele deelnemers, de betrokken werkgevers, als ook bij alle andere betrokkenen te voorkomen, dan wel tot een minimum te beperken.

De verantwoordelijkheid voor het informeren van de Autoriteit Persoonsgegevens wordt primair belegd bij de verantwoordelijken, indien er sprake is van een datalek. Discussie in deze is welke partij als primair verantwoordelijke kan worden aangemerkt. Degene die bijvoorbeeld de veroorzaker is van het lek, hoeft immers niet de partij te zijn bij wie het lek zich openbaart. We hebben daarbij niet alleen te maken met een juridische verantwoordelijkheid maar ook een morele verantwoordelijkheid. Wij adviseren om de veroorzaker van het lek primair verantwoordelijk te houden voor het melden en de constateerder moreel verantwoordelijk. Vanzelfsprekend mag van de betreffende partijen worden verwacht dat zij elkaar informeren. In deze adviesrapportage zal per risicogebied geen verantwoordelijke worden benoemd. Ditzelfde geldt ook voor de eventuele informatieverplichtingen richting de deelnemers/werknemers, opgelegd vanuit de wetgeving. Ook over deze informatieverplichting zal vanuit deze rapportage geen advies worden gegeven.

Aandachtspunt bij de communicatie aan anderen dan de deelnemer/werknemer, zoals een softwareontwikkelaar (SWO), is dat de communicatie in principe beperkt moet blijven tot de aard en strekking van het beveiligingsrisico of het datalek. De doelstelling van de informatie is immers het op de hoogte brengen van de situatie en hen betrekken bij de analyse en mogelijke oplossingsrichting. Bij het informeren van softwareontwikkelaars is het niet van

belang dat er geen of geen directe juridische relatie bestaat tussen hen en de betreffende pensioenuitvoerder of het fonds.

Datalek

Het begrip datalek toegelicht

Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie of persoon, zonder dat dit de bedoeling is van deze organisatie of persoon. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens.

We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens (zoals bedoeld in de Wbp[1], art. 13 en in de AVG[2], art. 4.1). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

De vervolgvraag die opkomt, is wat men verstaat onder verwerking? De AVG, art. 4.2 geeft een zeer ruime definitie van het begrip verwerken. De AVG verstaat hieronder een bewerking, of een geheel van bewerkingen, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Als alleen sprake is van een zwakke plek in de beveiliging, spreken we nog niet van een datalek. U hoeft van een zwakke plek in de beveiliging geen melding te doen aan de Autoriteit Persoonsgegevens. De meldplicht bij datalekken wordt hierna verder toegelicht.

Meldplicht datalekken

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat organisaties (zowel private als publieke organisaties) direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een datalek hebben geconstateerd. En soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

Kader

Iedereen heeft recht op eerbiediging en bescherming van zijn persoonlijke levenssfeer en een zorgvuldige omgang met zijn persoonsgegevens. De regels hiervoor zijn vastgelegd in de Wet bescherming persoonsgegevens (Wbp) en sinds mei 2016 ook in een Europese Algemene Verordening Gegevensbescherming (AVG 679/2016). Hierin staat dat u de persoonsgegevens die u verwerkt moet beveiligen tegen verlies en tegen onrechtmatige verwerking (Wbp art. 13 en AVG art. 32 lid 1). Alhoewel de Verordening onmiddellijke rechtskracht heeft en boven de Wpb uitgaat, krijgt iedere organisatie tot 25 mei 2018 de gelegenheid om de bedrijfsvoering in overeenstemming te brengen met de AVG. Op basis van de Wbp moet een datalek worden gemeld aan de Autoriteit Persoonsgegevens als het leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens (Wbp art. 34a lid 1 en AVG art. 33.1 en 34.1). Het datalek moet daarnaast ook worden gemeld aan de betrokkene indien het waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer (Wbp art. 34a lid 2, AVG art. 33).

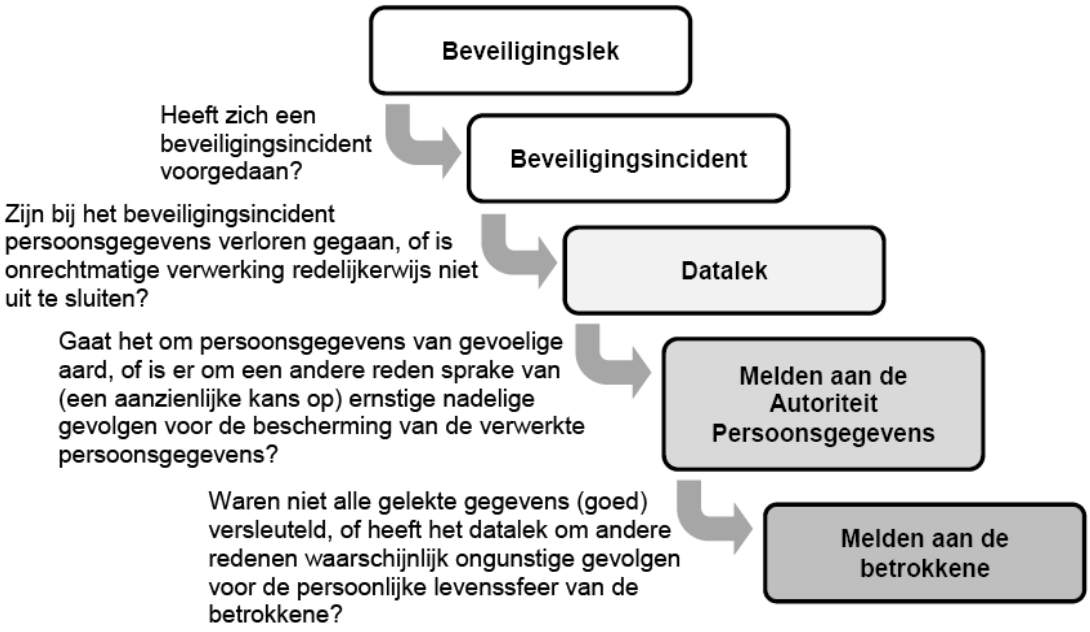
---

[1] Wbp: Wet bescherming Persoonsgegevens

[2] AVG: Algemene Verordening Gegevensbescherming, EU-verordening 679/2016

Afweging

Bij de beslissing of u een gebeurtenis die zich heeft voorgedaan moet melden aan de Autoriteit Persoonsgegevens, en eventueel daarnaast ook aan de betrokkene, moet u een aantal afwegingen maken. Het onderstaande schema geeft deze afwegingen weer.



Niet ieder datalek hoeft te worden gemeld aan de Autoriteit Persoonsgegevens. Volgens de wet moet u een melding doen aan de Autoriteit Persoonsgegevens als het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.

Een factor die hierbij een rol speelt is de aard van de gelekte persoonsgegevens. Als er persoonsgegevens van gevoelige aard zijn gelekt, dan is over het algemeen een melding noodzakelijk.

Bij persoonsgegevens van gevoelige aard moet u denken aan:

- Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp en artikel 9.1 AVG. Het gaat hierbij om persoonsgegevens over iemands 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 de financiële of economische situatie van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
- Gebruikersnamen, wachtwoorden en andere inloggegevens. De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar

de inloggegevens toegang toe geven. Onderdeel van de afweging is dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.

- Gegevens die kunnen worden misbruikt voor (identiteits)fraude. Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (bsn). Overigens is het verbod op de verwerking van het BSN conform artikel 24 Wbp niet opgenomen in de AVG. Nederland heeft echter de mogelijkheid om aanvullende voorwaarden te stellen aan het gebruik van identificatienummers.

Voorbeelden datalekken

Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker. Het is daarbij niet direct van belang of de data versleuteld is of niet, omdat niet uitgesloten kan worden dat een onbevoegde toegang tot de informatie kan hebben.

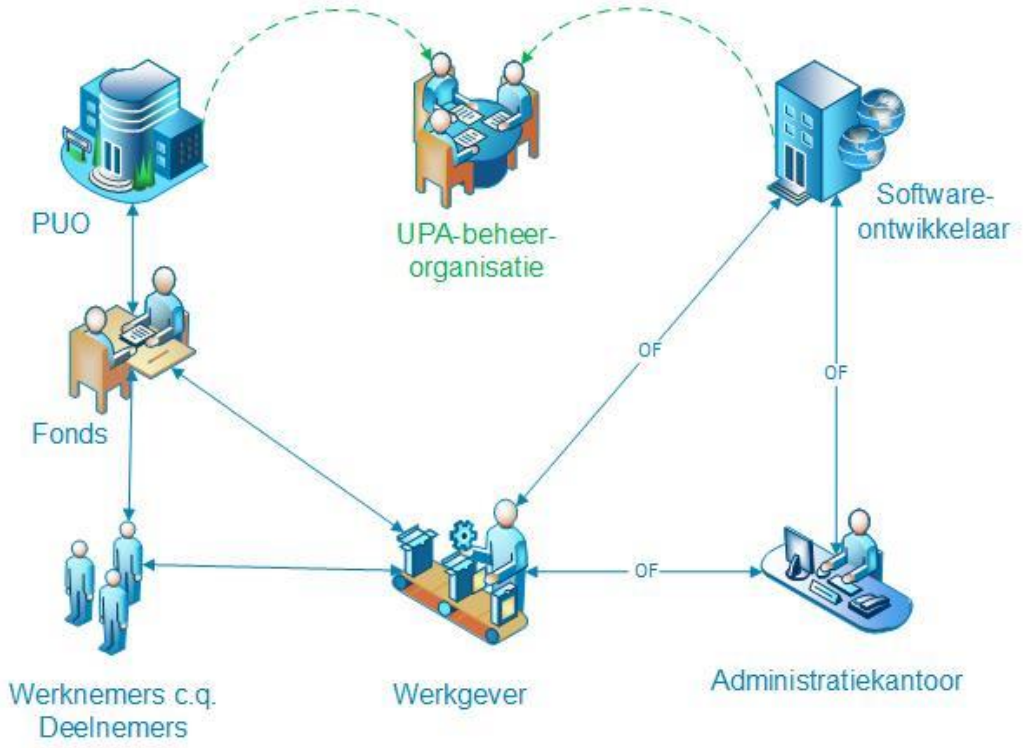
Beleidsregels meldplicht datalekken

De Autoriteit Persoonsgegevens heeft beleidsregels ten aanzien van meldplicht datalekken opgesteld. Deze beleidsregels zijn bedoeld om organisaties te helpen bij het bepalen of er sprake is van een datalek dat zij moeten melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

De Uniforme Pensioenaangifte (UPA)

Onderlinge relaties

In het kader van de UPA spelen een aantal organisaties en personen een rol. In onderstaande afbeelding zijn de relaties tussen de betrokken partijen weergegeven. Daarna volgt er een korte toelichting op de individuele rollen.



De pensioenuitvoeringsorganisatie (PUO) is verantwoordelijk voor de administratieve verwerking van de pensioengegevens voor de pensioenfondsen. De fondsen zijn de opdrachtgever voor de uitvoerder.

Het pensioenfonds is verantwoordelijk voor de data van de deelnemers. Het fonds geeft de opdracht aan de PUO voor bepaalde administratieve taken. Binnen de UPA gaat het hier om het incassoproces, het innen van premies en gegevens. Het fonds heeft middels het uitvoeringsreglement een overeenkomst met de aangesloten werkgevers. Het fonds heeft via het pensioenreglement een afspraak met de deelnemers. Binnen de kaders van dit document, wordt er geen onderscheid gemaakt tussen een OPF, BPF, e.d.

De werkgever heeft een arbeidsrechtelijke verhouding met de werknemer. Voor de loonbetaling moet de werkgever een salarisadministratie voeren. Hierbij kan hij gebruik maken van een administratiekantoor of serviceverwerker. Deze relatie is inzichtelijk gemaakt binnen de afbeelding die hierna is opgenomen bij UPA-dataflow. De relatie van de werkgever ten opzichte van het fonds is gebaseerd op het uitvoeringsreglement.

De werknemer heeft een arbeidsrechtelijke verhouding met de werkgever. Deze werknemer is deelnemer bij het fonds op basis de bepalingen in het pensioenreglement.

Een administratiekantoor voert in opdracht van de werkgever de salarisadministratie van die werkgever.

Voor de salarisadministratie wordt gebruik gemaakt van specifieke software, gericht op het berekenen van betalingen en inhoudingen en het vaststellen van het netto te betalen loon. Vanuit deze software wordt de overheid en pensioenuitvoerders via aangifteberichten zoals een UPA voorzien van informatie die zij voor hun uitvoering nodig hebben. De inzender van deze aangiftebestanden, kan per salarissysteem verschillen. Soms worden de bestanden aangeboden door de werkgever zelf, maar soms kan dit ook vanuit de SWO aangeleverd worden. De salarissoftware kan worden gebruikt door de zelfadministrerende werkgever of zijn administratiekantoor.

Serviceverwerkers zijn niet opgenomen binnen deze afbeelding. Dit zijn softwarehuizen, die afhankelijk van de afspraken met de werkgever diensten aanbieden welke kunnen variëren van een centraal rekencentrum tot volledige business proces outsourcing. Afhankelijk van deze maatwerkafspraken kunnen zij binnen deze afbeelding zowel worden gezien als een softwareontwikkelaar als een administratiekantoor.

De UPA-beheerorganisatie is een orgaan namens de PUO's en de gezamenlijke SWO's, waarin zij via een afvaardiging zijn vertegenwoordigd. De beheerorganisatie bepaalt en onderhoudt de gegevensspecificaties van het UPA-bericht.

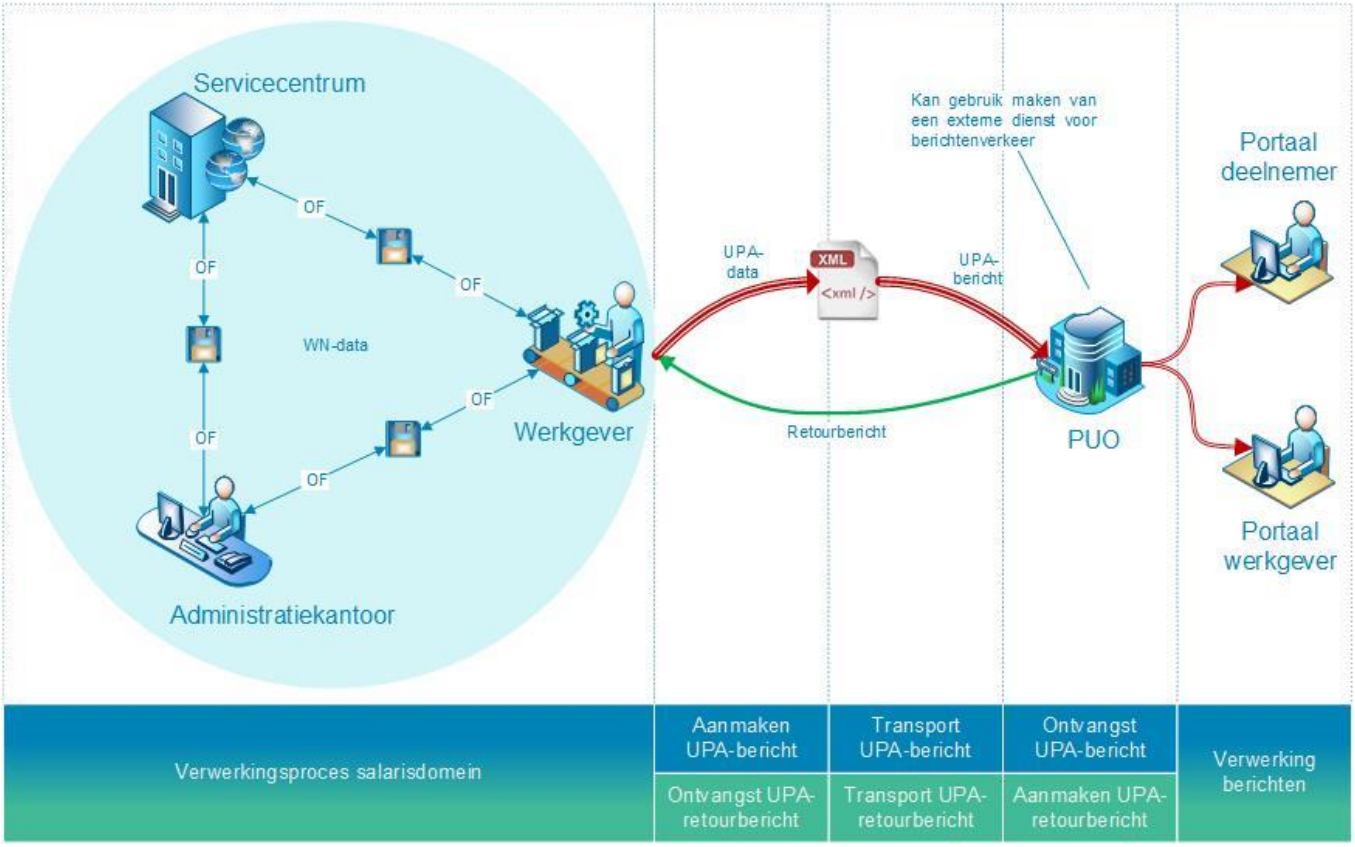
UPA-dataflow

De UPA-data ondergaat een weg in de keten. De gegevens zullen worden vastgelegd binnen het salarisdomein. Dat kan door de werkgever worden gedaan, maar hij kan hiervoor ook gebruik maken van de diensten van een administratiekantoor of serviceverwerker. Door of namens de werkgever zal een UPA-aangifte worden samengesteld en getransporteerd. Na ontvangst zal de data worden verwerkt bij de PUO.

Diverse serviceverwerkers zijn ook softwareontwikkelaar, maar dat is een andere rol. Deze marktpartijen ontwikkelen eigen software en stellen die beschikbaar via een centraal rekencentrum aan de werkgever of het administratiekantoor en zullen doorgaans vanuit dat rekencentrum de UPA-aangiften aanleveren bij een pensioenuitvoerder. Vanwege hun rol als centraal rekencentrum zijn zij apart weergegeven in de afbeelding van de dataflow. In hun rol

als softwareleverancier maken zij geen deel uit van deze afbeelding, maar maken zij deel uit van de beheerorganisatie. Bij de beheerorganisatie komt hun rol dan overeen met die van leveranciers van personeels- en salarissystemen en erp-oplossingen.

In de volgende afbeelding is de flow van de data weergegeven.



Risicogebieden in de UPA procesonderdelen

In deze paragraaf worden voor diverse procesonderdelen een aantal risico's beschreven. Deze risico's zijn nader toegelicht en per proces worden de betrokkenen benoemd en beknopt enkele adviezen gegeven.

Het verwerkingsproces van de salarisadministratie, die in de eerder getoonde afbeelding met het blauwe vlak is aangegeven, valt buiten de processen die in dit document zijn beschreven en wordt hieronder niet verder behandeld.

Voor de volgende processen zijn een aantal risico's uitgewerkt:

- Aanmaken UPA-bestand;
- Transport UPA-bestand;
- Ontvangst UPA-bestand;
- Verwerken UPA-bestand;
- Aanmaken UPA-retourbericht;
- Transport UPA-retourbericht;
- Ontvangst UPA-retourbericht;
- Verwerken UPA-retourbericht.

Deze processen zijn terug te vinden in de hiervoor beschreven dataflow.

De geïnventariseerde risico's zijn:

- Verloren datadrager;
- Ongeautoriseerde toegang tot het UPA- en retourbericht;
- Foutief identificerend gegeven;
- Onjuiste autorisatie binnen het portaal van de PUO.

Per risico wordt per procesdeel beschreven welke partijen betrokken zijn. Bij alle in dit document benoemde risico's zijn meerdere partijen betrokken en daarom wordt ieder risico afgehandeld alsof deze zich buiten de eigen organisatie geopenbaard kan hebben. Mede hierdoor wordt in beginsel ieder risico als 'hoog' gedefinieerd. Dit kan na een nadere analyse worden afgewaardeerd naar een lager niveau. Uitgangspunt daarbij is dat men bij een beveiligingsincident eerst uit moet gaan van het meest ongunstige scenario. De verantwoordelijke(n) zullen op basis van de feitelijke situatie een goede duiding moeten geven van de impact en de juiste passende maatregelen moeten nemen, gericht op het voorkomen van schade, het herstel van (toekomstige) schade en communiceren naar alle betrokkenen. Indien van toepassing dienen ook de betrokken deelnemers/werknemers persoonlijk te worden geïnformeerd.

Verloren data en/of datadrager

Er is een data(drager) verloren geraakt, waarvan de data niet of onvoldoende versleuteld is. Omdat versleuteling niet voldoet aan de norm dient naast de Autoriteit ook de betrokkene(n)/klanten te worden geïnformeerd. De Europese verordening 611/2013, art. 4 geeft een nadere invulling aan een adequate versleuteling. Opvolging daarvan blijft echter een eigen verantwoordelijkheid.

Processen	Betrokkenen	Advies
Aanmaken UPA-bestand	Werkgever; administratiekantoor; servicecentrum.	Interne procedure nagaan en passende maatregelen nemen. Na het opnieuw aanmaken van het bestand, kan het alsnog worden verzonden.
Transport UPA-bestand	Werkgever; administratiekantoor; servicecentrum.	De oorzaak en de datadrager achterhalen. Passende maatregelen nemen om herhaling in de toekomst te voorkomen. Bestanden met persoonlijke gegevens mogen uitsluitend via beveiligde verbindingen worden aangeleverd bij een PUO. Het is verstandig dat de PUO's en de SWO's afstemming hebben over de te nemen maatregelen. Alle betrokkenen moeten worden geïnformeerd, inclusief de Autoriteit Persoonsgegevens. Indien de oorzaak ligt binnen de salarissoftware, moet ook de SWO worden betrokken in de communicatie.

Processen	Betrokkenen	Advies
Ontvangst UPA-bestand	Werkgever; administratiekantoor; servicecentrum; PUO	De oorzaak achterhalen en passende maatregelen nemen; Het is verstandig dat de PUO's en de SWO's afstemming hebben over de te nemen maatregelen. Indien de machtiging van de inzender bij de PUO niet op orde is, moet deze worden aangebracht. Indien mogelijk dient de machtiging datumafhankelijk te zijn in verband met de overdracht van werkzaamheden aan een andere inzender.
Verwerken UPA-bestand	PUO	n.v.t.
Aanmaken retourbericht	PUO	n.v.t.
Transport retourbericht	Werkgever; administratiekantoor; servicecentrum.	De oorzaak en de datadrager achterhalen. Passende maatregelen nemen om herhaling in de toekomst te voorkomen. Bestanden met persoonlijke gegevens mogen uitsluitend via beveiligde verbindingen worden verzonden vanuit een PUO. Om risico's te beperken moet persoonlijke informatie in het retourbericht tot een minimum worden beperkt. Alle betrokkenen moeten worden geïnformeerd, inclusief de Autoriteit Persoonsgegevens.
Ontvangst retourbericht	Werkgever; administratiekantoor; servicecentrum; PUO	De oorzaak achterhalen en passende maatregelen nemen. Het is verstandig dat de PUO's en de SWO's afstemming hebben over de te nemen maatregelen. Om risico's te beperken moet persoonlijke informatie in het retourbericht tot een minimum worden beperkt. Indien de machtiging van de inzender bij de PUO niet op orde is, moet deze worden aangebracht. Indien mogelijk dient de machtiging datumafhankelijk te zijn in verband met de overdracht van werkzaamheden aan een andere inzender.
Verwerken retourbericht	Werkgever; administratiekantoor; servicecentrum.	Interne procedure nagaan en passende maatregelen nemen.

Ongeautoriseerde toegang tot het UPA- en retourbericht

Databestand waar ongeautoriseerden toegang toe hebben. Het is hierbij niet van belang of de oorzaak ligt bij een foutieve gebruikershandeling, een verstoring binnen de techniek of frauduleuze handelingen vanuit de interne organisatie of van buiten de organisatie.

Processen	Betrokkenen	Advies
Aanmaken UPA-bestand	Werkgever; administratiekantoor; servicecentrum.	Interne procedure nagaan en passende maatregelen nemen. Functiescheiding invoeren, zodat alleen geautoriseerde personen nog toegang hebben tot de gegevens.
Transport UPA-bestand	Werkgever; administratiekantoor; servicecentrum.	Beveiliging aanscherpen. Werkgever / PUO / Autoriteit inlichten
Ontvangst UPA-bestand	PUO	Autorisatie aanpassen en functiescheiding toepassen.
Verwerken UPA-bestand	PUO	Vermoedelijk ligt de oorzaak bij de overdracht van de werkgeveradministratie aan een andere servericeverwerker of administratiekantoor. De PUO wordt hierom aangeraden om een datumafhankelijke autorisatie te ondersteunen. Hierdoor kan de voormalige dienstverlener zijn werkzaamheden afronden en kan de nieuwe dienstverlener de nieuwe aangiften insturen. De PUO's en de SWO's zullen de technische voorzieningen hiervoor moeten bespreken en afstemmen.
Aanmaken retourbericht	PUO	Interne procedure nagaan en passende maatregelen nemen. Functiescheiding invoeren, zodat alleen geautoriseerde personen nog toegang hebben tot de gegevens.
Transport retourbericht	PUO	Beveiliging aanscherpen Werkgever / PUO / Autoriteit inlichten
Ontvangst retourbericht	Werkgever; administratiekantoor; servicecentrum	De software dient te borgen, dat alleen retourberichten kunnen worden verwerkt, waar ook een UPA-bericht tegenover staat.
Verwerken retourbericht	Werkgever; administratiekantoor; servicecentrum.	Autorisatie aanpassen en functiescheiding toepassen.

Foutief identificerend gegeven

Door een invoer- of softwarefout geeft het salarispakket een verkeerd identificerend gegeven (burgerservicenummer, loonheffingennummer, aansluitnummer bij het fonds) door van een werkgever. Voorbeeld: Het instellingsnummer is de unique identifier voor een fonds. Indien de UPA-aangifte met een verkeerd, doch bestaand instellingsnummer wordt aangeleverd, dan worden de persoonsgegevens van een werkgever die niet is aangesloten bij dat specifieke fonds ten onrechte toch verwerkt door het fonds c.q. door de betrokken PUO.

Processen	Betrokkenen	Advies

Processen	Betrokkenen	Advies
Aanmaken UPA-bestand	Werkgever; administratiekantoor; servicecentrum.	Niet versturen, maar het identificerend gegeven aanpassen en daarna versturen. Binnen het salarissysteem mag het niet mogelijk zijn, om een identificerend gegeven te wijzigen, zolang hierop een aangiftehistorie aanwezig is. Fouten op dit vlak kunnen slechts voorkomen worden, door binnen het administratieve proces altijd uit te gaan van het oorspronkelijke document waarop dit gegeven door het fonds of vanuit de overheid wordt gecommuniceerd. Denk daarbij aan een aansluitbrief of een kopie identiteitsbewijs.
Transport UPA-bestand	Werkgever; administratiekantoor; servicecentrum.	Beveiliging aanscherpen Werkgever / PUO / Autoriteit inlichten Herstelactie Opnieuw (goed) aanleveren
Ontvangst UPA-bestand	PUO	De PUO dient dit bestand, of bepaalde gegevens uit dat bestand niet te accepteren. Er wordt aangeraden om bij aflevering bij de PUO, direct te controleren op een tweede identificerend gegeven, zoals de combinatie van een instellingsnummer en een loonheffingennummer. Vanuit de salarisadministratie zullen correcties moeten worden aangeleverd. De PUO mag niet via interventie een correctie uitvoeren, omdat daarmee de bron van de data gecorrigeerd wordt. Alle betrokkenen binnen de aangifteketen moeten worden geïnformeerd, inclusief de SWO's. Diverse SWO's hebben immers ook de rol van servicecentrum.
Verwerken UPA-bestand	PUO	Passende maatregelen nemen om de oorzaak te achterhalen en de gevolgen te herstellen. De maatregelen zijn echter reactief van aard, omdat de oorzaak binnen de voorgaande processen zal liggen. Alle betrokkenen binnen de aangifteketen moeten worden geïnformeerd, inclusief de SWO's. Diverse SWO's hebben immers ook de rol van servicecentrum. Het fondsbestuur wordt door de PUO op de hoogte gebracht, welke kan besluiten om de deelnemers te informeren. Het datalek moet tevens worden gemeld bij de Autoriteit Persoonsgegevens.
Aanmaken retourbericht	N.v.t.	Retourberichten zijn een reactie op ingezonden berichten. Onjuiste identificering wordt vooralsnog niet voorzien.
Transport retourbericht		

Processen	Betrokkenen	Advies
Ontvangst retourbericht		
Verwerken retourbericht		

Onjuiste autorisatie binnen portaal PUO

Het gaat hier om de ongeautoriseerde toegang op het portaal van de PUO, nadat de gegevens door de pensioenuitvoerder zijn verwerkt. Dit kan worden veroorzaakt, doordat de werkgever wisselt van administratiekantoor of servicecentrum. Er is hierdoor een tijdelijke overgangssituatie waarbij beide administratiekantoren/servicecentra geautoriseerd zijn voor de gegevens van deze werkgever op het werkgeverportaal van de PUO. Het wordt de PUO aanbevolen om een sluitend proces rondom de portaalautorisatie in te richten.

Processen	Betrokkenen	Advies
Aanmaken UPA-bestand	N.v.t.	
Transport UPA-bestand	N.v.t.	
Ontvangst UPA-bestand	Werkgever, administratiekantoor, servicecentrum, PUO.	Oorzaak achterhalen en passende maatregelen nemen. Daarbij wordt aangeraden om een datumafhankelijke toegangsscheiding te faciliteren, zodat bij een overdracht van dienstverlener de voormalige dienstverlener de werkzaamheden kan afronden. De PUO's en de SWO's zullen de technische voorzieningen hiervoor moeten bespreken en afstemmen. Bij constatering van het datalek alle betrokkenen informeren, inclusief de SWO's wanneer het een structurele oorzaak blijkt te hebben.
Verwerken UPA-bestand	PUO	Oorzaak achterhalen en passende maatregelen nemen. Bij constatering van het lek de werkgever en het administratiekantoor informeren. Indien de oorzaak structureel blijkt te zijn is het verstandig om ook de SWO mee te nemen in de communicatie.
Aanmaken retourbericht	PUO	Interne procedure nagaan en passende maatregelen nemen. Functiescheiding invoeren, zodat alleen geautoriseerde personen nog toegang hebben tot de gegevens.
Transport retourbericht	PUO	Betreft het uitlezen van het retourbericht binnen het portaal. Oorzaak achterhalen en passende maatregelen nemen.
Ontvangst retourbericht	N.v.t.	Deze processen vallen buiten de afhandeling van het portaal.
Verwerken retourbericht		

<lege pagina>