Auditreglement UWV Gegevensdiensten

nadere uitwerking van het artikel uit de overeenkomst inzake Audits en periodiek overleg

Dit auditreglement maakt deel uit van de tussen UWV en Afnemer gesloten overeenkomst.

Afnemers ontvangen gegevens van UWV. UWV en Afnemer sluiten hiertoe een overeenkomst, waarin de voorwaarden staan waaronder Afnemers de gegevens mogen ontvangen en gebruiken. Onderdeel van de overeenkomst is een auditverplichting. Deze auditverplichting wordt middels het auditreglement nader ingevuld.

Resultaat van de audit is een Assurance-rapport. Hiermee wordt bedoeld een door Afnemer aan UWV te verstrekken Assurance-rapport van de auditor volgens Standaard 3000 (NBA) dan wel Richtlijn 3000 (NOREA), conform het bij dit reglement opgenomen model.

DEEL 1 ALGEMEEN DEEL

Artikel 1 Auditor

De audit wordt uitgevoerd onder leiding van een (interne of externe) auditor die geregistreerd staat als:

a. Certificerend AA-accountant bij NBA
b. RA-accountant bij NBA
c. RE- Register EDP-auditor bij NOREA

Artikel 2 Uitvoeren jaarlijkse audit

1. Afnemer voert eenmaal per kalenderjaar een audit uit of laat deze uitvoeren.
2. Op deze audit is dit auditreglement van toepassing.
3. De audit wordt uitgevoerd op basis van het referentiekader zoals beschreven in deel 2 van dit auditreglement.

Artikel 3 Assurance-rapport

1. Het Assurance-rapport bevat in ieder geval de volgende elementen:
a. Werkwijze en werkzaamheden van de auditor
b. Het gehanteerde normenkader
c. De bevindingen
d. Oordeel over de getroffen beheersmaatregelen
2. De auditor -zoals genoemd in artikel 1 van dit reglement- ondertekent het Assurance-rapport.
3. Indien de conclusie uit het Assurance-rapport daartoe aanleiding geeft, stelt Afnemer een verbeterplan op. De te nemen maatregelen en een planning maken onderdeel uit van dit verbeterplan. Afnemer doet het aan UWV aan te reiken Assurance-rapport vergezeld gaan van het hiervoor bedoelde verbeterplan.

Artikel 4 Tussentijdse audit

Indien de bevindingen uit het Assurance rapport daartoe aanleiding geven, kan UWV Afnemer verplichten om een tussentijdse audit uit te voeren.

Artikel 5 Opschorting en opzegging

De bepalingen uit de algemene voorwaarden omtrent opschorting van de gegevenslevering en opzegging van de overeenkomst zijn onverminderd van toepassing op het auditreglement.

DEEL 2 UWV REFERENTIEKADER

Dit referentiekader is principle based van aard. De auditor dient in afstemming met Afnemer en passend bij de bedrijfsvoering en conform de gestelde eisen in de overeenkomst van de gegevenslevering deze principes nader uit te werken in een specifiek werkprogramma, toe te passen op het object van onderzoek. Hierbij dient hij, naast opzet en bestaan van maatregelen, ook de werking van de getroffen maatregelen te beoordelen.

I Algemeen beleidscontext

I –1 Doelbinding

De van UWV ontvangen gegevens worden slechts voor de uitvoering van de in de overeenkomst vastgelegde doeleinden gebruikt.

I –2 Gegevenslimitatie

Afnemer vraagt niet meer gegevens op dan strikt noodzakelijk voor de uitvoering van de in de overeenkomst vastgelegde doeleinden. Indien er meer gegevens worden verstrekt, worden deze bij ontvangst/kennisneming daarvan vernietigd onder vermelding hiervan aan UWV Gegevensdiensten.

I –3 Informatiebeveiligingsbeleid

Afnemer dient over een actueel informatiebeveiligingsbeleid te beschikken waarin aandacht wordt besteed aan:

- Eisen gesteld vanuit de Algemene verordening gegevensbescherming (AVG)
- Richtlijnen voor omgang met vertrouwelijke informatie;
- Het bewaren en het transporteren van gegevensdragers met persoonsgegevens;
- Geheimhoudingsplicht van personeel en externe medewerkers;
- Het veilig afvoeren van opslagmedia met bedrijfsgevoelige of privacygevoelige informatie.

I –4 Gegevensverstrekking

Afnemer mag alleen UWV- gegevens verstrekken aan derden als UWV daar formeel toestemming voor heeft gegeven.

I –5 Verwerker

Het inschakelen van een Verwerker door Afnemer dient te geschieden op basis van een contractuele vastlegging waarbij de Verwerker dient te voldoen aan het auditreglement.

- Afnemer en Verwerker hebben conform artikel 28, derde lid AVG een verwerkersovereenkomst gesloten of een andere (schriftelijk vastgelegde) rechtshandeling verricht waardoor er een verbintenis bestaat tussen Afnemer en Verwerker;
- In de overeenkomst tussen Afnemer en Verwerker staan afspraken over de uitvoering van verwerkingen van (UWV)-gegevens;
- Voor de verwerking van de (UWV-)gegevens heeft de Verwerker adequate organisatorische en technische beveiligingsmaatregelen getroffen.

I –6 Geheimhouding

Zowel medewerkers van Afnemer als externe functionarissen zijn formeel verplicht tot geheimhouding (bijvoorbeeld via een verklaring, contract of aanstelling).

IIA Specifiek beleidscontext

IIA –1 Beveiliging van de UWV -gegevens

De eisen uit het informatiebeveiligingsbeleid dienen te zijn toegespitst op de beveiliging van de omgeving waarin de door UWV verstrekte gegevens worden opgeslagen, geraadpleegd en bewerkt. Aandachtspunten zijn beveiliging ten aanzien van autorisaties, applicaties en gegevensverwerking.

II B Uitvoering

IIB –1 Logische Toegangsbeveiliging: Identificatie & Authenticatie

De gebruikers van, de door Afnemer gebruikte en beheerde, applicaties dienen op een unieke wijze te worden geïdentificeerd en geauthentiseerd om te garanderen dat deze applicaties slechts door geautoriseerden toegankelijk zijn. Aandachtspunten hierbij zijn

Identificatie- en Authenticatiemechanisme

- De identificatie- en authenticatiemechanismen zijn afgestemd op de raadpleging en bewerking van vertrouwelijke van informatie;
- Het voorzien van accounts van een niet triviaal en niet default wachtwoord;
- Het gebruik van persoonsgebonden/unieke gebruikersaccounts is verplicht;
- Herleidbaarheid van accounts naar één persoon (eindgebruiker en beheerder);
- Het automatisch blokkeren van tijdelijke accounts;
- Het blokkeren van eventuele standaard accounts;
- Het hanteren van een wachtwoordbeleid m.b.t. karakterlengte, geldigheidsduur, complexiteit, lock-out strategie en historie;
- Het verplicht stellen van het wijzigingen van Initiële wachtwoorden bij de eerste keer inloggen.

IIB-2 Logische Toegangsbeveiliging: Autorisatie

Autorisaties tot applicaties dienen te worden toegekend aan geïdentificeerde en geauthentiseerde gebruikers conform de autorisatieprofielen en autorisatieproces om de uitvoering van de juiste acties binnen de applicatie te kunnen garanderen. Aandachtspunten hierbij zijn

Identificatie Autorisatieprofielen

- Functies zijn geïdentificeerd die met de gegevens mogen omgaan;
- Identificatie van de noodzakelijke functiescheidingen;
- Identificatie van de noodzakelijke autorisatieprofielen;
- Autorisatieprofielen goedgekeurd door het management;
- Inrichting van autorisaties op basis van RBAC (Rol Based Access Control) voor alle type gebruikers (eindgebruikers & beheerders).

Autorisatieproces

- De aanvraag, toekenning en intrekken van autorisaties conform de voorgeschreven (autorisatie) procedure.

IIB-3 Koppelingen tussen Applicaties

Afnemer dient te voorkomen dat de door UWV geleverde gegevens worden verspreid over informatiesystemen die niet noodzakelijk zijn voor de uitvoering van de in de overeenkomst vastgelegde doeleinden.

IIB-4 Gegevensverwerking

Het verwerken(inlezen) van de door UWV geleverde gegevens in het domein van Afnemer vindt plaats conform vastgelegde en goedgekeurde procedures. Aandachtpunten zijn:

- Verwerking vindt plaats door geautoriseerde functionarissen;
- De procedure waarborgt dat eventuele voor de bedrijfsvoering niet noodzakelijke en/of juridisch niet toegestane gegevens bij ontvangst dan wel kennisgeving daarvan worden vernietigd.

II C Controles t.av. Applicaties

IIC-1 Handelingen van functionarissen

Afnemer dient een formeel proces te hebben ingericht voor het periodiek controleren of toegangsrechten nog conform het "need to know" en "need to have" principe zijn toegekend.

IIC-2 Historie (Logging)

De Applicatie dient zodanig te zijn ontwikkeld dat verdachte gebeurtenissen en eventuele schendingen van de security – eisen worden gesignaleerd en vastgelegd. Aandachtspunten hierbij kunnen zijn:

- Logging van verkeersstromen en activiteiten;
- Rapportage van gesignaleerde incidenten (ongeautoriseerde toegang of misbruik van informatiesystemen);
- Bewaartermijnen van logbestanden.

III Beheerprocessen

III-1 Wijzigingenbeheer

Alle wijzigingsverzoeken dienen te verlopen volgens een formele wijzigingsprocedure, waaronder ook die op het gebied van identificatie, authenticatie en autorisatie.