Shared Expertise B.V.

(laatste update:18-05-2018)

Verwerking

Registratienummer	SE01	
Naam verwerking	Casemanagement	
Verantwoordelijke	Shared Expertise B.V.	
	James Wattstraat 11 1817 DC Alkmaar Nederland	Postbus 216 1800 AE Alkmaar Nederland
Doel(en) van verwerking	1. Aangaan en uitvoeren van een dienstverleningsovereenkomst casemanagement. Hieronder valt onder meer het beoordelen en accepteren van (potentiële) cliënten, alsmede het beheren van de uit de overeenkomst voortvloeiende relaties; 2. Advisering over de inkomenspositie en de mogelijkheden van de werknemer om de werkhervatting te bevorderen. 3. Begeleiden van de werkgever op het gebied van re-integratie en inzetbaarheid van arbeidsongeschikte werknemers; 4. Verlenen van service in verband met genoemde overeenkomst; 5. Verantwoorde uitoefening van de bedrijfsdoelstellingen van de organisatie mede ten behoeve van samenwerkingsverbanden; 6. Genereren van management- en beleidsinformatie, onder meer ten behoeve van de kwaliteit van de dienstverlening alsmede ten behoeve van het bepalen van algemene strategie en beleid; 7. Voorschriften uit wet- en regelgeving. Hiermee wordt bedoeld het voldoen aan wettelijke verplichtingen, maar ook wettelijk verplichte informatieverstrekking aan toezichthouders en opsporingsautoriteiten valt hieronder; 8. Bijhouden van hoe en wanneer wij contact met betrokkene hebben, bijvoorbeeld ter verbetering van de communicatie, als bewijs, of voor training van onze medewerkers. In dit kader kunnen wij ook telefoongesprekken opnemen.	
Grondslag(en) van verwerking	• De betrokkene heeft voor de verwerking zijn ondubbelzinnige toestemming verleend; • De gegevens zijn noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst; • De gegevens zijn noodzakelijk om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is; • De gegevens zijn noodzakelijk voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt. Het gerechtvaardigd belang betreft het van belang van werkgever en werknemer in het kader van re-integratie en inzetbaarheid van arbeidsongeschikte werknemers.	

Betrokkene(n)

Hoedanigheid betrokkene	**Categorieën van persoonsgegevens**
Werkgever	NAW-gegevens
	Telefoon, e-mail
	Bedrijfsgegevens
	KvK-nummer
	Polis –en schadenummer
	Bankrekeningnummer en betaalgegevens
	Contactpersoon (naam en contactgegevens)
	Voor communicatie benodigde gegevens
Hoedanigheid betrokkene	**Categorieën van persoonsgegevens**
Werknemer	NAW-gegevens
	Telefoon, email

	Geslacht
	Geboortedatum
	Soort dienstverband
	Fulltime of parttime en uren per week werkzaam
	Functie
	Salaris / inkomensgegevens
	Datum in dienst
	Datum uit dienst
	1e ziektedag
	Percentage arbeidsgeschiktheid
	Vangnet UWV of no-risk polis aanwezig
	Ongeval ja/nee
	Interventies
	Opbouwschema / werkhervattingafspraken
	Plan van aanpak inzake re-integratie
	Prognose bedrijfsarts inzake verzuimduur
	Hersteldatum
	Niet medische gezondheidsgegevens die nodig zijn om de re-integratie(mogelijkheden) te bevorderen
	BSN (uitsluitend gebruikt in communicatie met UWV)
Hoedanigheid betrokkene	**Categorieën van persoonsgegevens**
Externe Deskundigen (Waaronder Arbodienstverlener, Interventiebedrijf)	NAW-gegevens
	Telefoon, e-mail
	Bedrijfsgegevens
	Bankrekeningnummer en betaalgegevens
	Declaraties en declaratiegegevens
	Voor communicatie benodigde gegevens

Ontvangers

	Categorieën van (mogelijke) ontvangers	**Doel(en)** (zie de eerste tabel 'Verwerking' bij 'Doeleind(en) verwerking voor de betekenis van de nummers)
Intern	Medewerkers Shared Expertise	1, 2, 3, 4
	Leidinggevende Shared Expertise	1, 2, 3, 4, 5, 6, 7, 8
	Categorieën van (mogelijke) ontvangers	**Doel(en)**
Extern binnen de holding	Internal Auditer, Risk officer & Compliance officer Holding	5
	Afdeling BI en Reporting	6
	Functionaris gegevensbescherming	5
	Categorieën van (mogelijke) ontvangers	**Doel(en)**
Extern buiten de holding	Betrokkene zelf	1, 2, 3, 4
	(Gevolmachtigde van) verzekeraar	5, 6
	Werkgever	1, 2, 3, 4
	Verwerkers, die de organisatie ondersteuning bij de uitvoering van haar werkzaamheden, waaronder softwareleverancier	1, 2, 3, 4
	Andere met de verantwoordelijke samenwerkende organisaties, één en ander ten behoeve van de uitvoering van de dienstverleningsovereenkomsten	1, 2, 3, 4
	Externe deskundigen zoals arbodienstverlener en interventiebedrijf	1, 2, 3, 4
	Personen en instanties die op grond van wettelijke verplichting(en) geïnformeerd moeten of mogen worden	7
	Klachtinstanties	1
	Belangenbehartigers van de betrokkene of wederpartij (bijvoorbeeld een advocaat of schuldsaneringsbureau)	1

Doorgifte

Binnen EU	Ja

Buiten EU	Nee
Internationale organisaties	Nee
Passend	N.v.t.

Bewaartermijnen

Persoonsgegevens worden 7 jaar bewaard, te rekenen vanaf de einddatum van de actieve relatie met betrokkene. Dit kan de einddatum zijn van de verzekering of –indien dat later is- de einddatum van het schadedossier of het financiële dossier. De bewaartermijn van 7 jaar is gebaseerd op de wettelijke bewaarverplichting van onze administratie. Soms zijn wij wettelijk verplicht om persoonsgegevens langer te bewaren. We houden ons dan aan de wettelijke termijn.

Nadat de toepasselijke bewaartermijn is verstreken, zullen wij de persoonsgegevens anonimiseren. Dit betekent dat de bij ons aanwezige persoonsgegevens niet meer te herleiden zijn naar de betrokkene als individu.

Algemene beschrijving technische en organisatorische beveiligingsmaatregelen

De bescherming van persoonsgegevens valt onder het informatiebeveiligingsbeleid van de organisatie. Dit informatiebeveiligingsbeleid is gebaseerd op negen pijlers:

- risicoanalyses, gericht op het bepalen van een beveiligingsclassificatie voor een (business)applicatie en eisen voor specifieke application controls;
- onderhouden van een basisbeveiligingsniveau voor de werkstations, netwerken, servers en storage. Hierbij valt te denken aan clear screen policy (schermbeveiliging), cryptografische versleuteling bij data-uitwisseling met externe partijen; beveiligde serverruimte; bescherming tegen kwaadaardige software.
- logische toegangsbeveiliging, gericht op het onderhouden van een set van regels voor het verlenen van toegang tot netwerk- en computersystemen, waaronder beveiliging van het netwerk middels een inlogprocedure (persoonlijke inlognaam en wachtwoord waarbij wachtwoorden periodiek dienen te worden gewijzigd);
- fysieke beveiliging, gericht op het weren van onbevoegden (toegangsbeveiliging en fysieke beveiliging van gebouw en omgeving);
- integriteitmanagement, gericht op het vaststellen van de betrouwbaarheid van het personeel bij het in dienst nemen van personeel, tijdens de uitvoering van het dienstverband en het einde dienstverband;
- bedrijfscontinuïteitsplannen met betrekking tot informatie in geval van calamiteiten (waaronder maken van back-ups);
- Incidentenmanagement, gericht op de registratie, analyse, escaleren, oplossen en voorkomen van beveiligingsincidenten.
- Autorisatiemanagement, gericht op het voorkomen van ongeoorloofde toegang tot applicaties en onderliggende data.
- Awareness, om de medewerkers regelmatig te wijzen op de rol die zij zelf spelen in de informatiebeveiliging en bescherming van de persoonsgegevens (o.a. Clean desk policy).