

Privacybescherming Stichting Kringloopbedrijf Het Warenhuis 2025

Kern

Bij Stichting Kringloopbedrijf Het Warenhuis (verder Het Warenhuis) werken mensen met en zonder afstand tot de arbeidsmarkt. De afstand tot de arbeidsmarkt is tijdelijk of blijvend en kan onder andere veroorzaakt worden door een lichamelijke, verstandelijke of psychische reden of een combinatie van deze. Ook een gebrek aan (taal)vaardigheden of arbeidsritme komt voor. De populatie met een dergelijke afstand is groot; in 2025 gaat het om ruim 100 mensen.

Daarnaast is er een onderscheid te maken tussen mensen met en zonder betaald dienstverband bij Het Warenhuis.

Om voor mensen met een afstand tot de arbeidsmarkt een veilige en op maat gemaakte werkomgeving te kunnen creëren is het nodig om, met toestemming van de persoon in kwestie, een aantal bijzondere persoonsgegevens vast te leggen.

Daarnaast verleent Het Warenhuis een aantal diensten aan klanten: het ophalen en/of bezorgen van goederen en het uitlenen van een aanhangwagen. Om deze dienstverlening mogelijk te maken worden enkele gegevens genoteerd en bewaard. Ook wordt een deel van het gemeentelijke Fiets Fout = Fiets Weg-beleid door Het Warenhuis uitgevoerd. In het kader hiervan worden gegevens verzameld om te voldoen aan wettelijke verplichtingen.

De pijlers waarop de privacybescherming rust:

- Het doel van gegevensverzameling
- De (soort) verzamelde gegevens
- Toestemming voor gegevensverzameling
- Gegevensbeveiliging; beperkte toegang tot gegevens
- Bewaartermijnen

Deze richtlijn kent drie delen: deel 1 betreft medewerkers van Het Warenhuis, deel 2 betreft klanten van Het Warenhuis en deel 3 betreft geregistreerde personen in het kader van de uitvoering van het gemeentelijke Fiets Fout = Fiets Weg-beleid.

DEEL 1: MEDEWERKERS

Het doel van gegevensverzameling

De verzameling van (persoons)gegevens vindt plaats tijdens een intakegesprek dat elke medewerker krijgt. Alle gegevens worden verstrekt met toestemming van de toekomstige medewerker.

Allereerst wordt de identiteit van de medewerker vastgelegd door een aantal identificerende gegevens. Wanneer toestemming hiervoor wordt geweigerd kan inschrijving niet plaatsvinden en komt geen werkovereenkomst tot stand. Een uitzondering hierop is het e-mailadres. Dit wordt al dan niet verstrekt en dient uitsluitend om toegang te verschaffen tot het HR-systeem.

Tijdens de intake wordt ook een aantal bijzondere persoonsgegevens gevraagd om de werkplek voor de medewerker zo veilig mogelijk te maken en de

begeleiding op de werkvloer aan te kunnen passen aan de persoonlijke behoeften van de medewerker. Weigering om deze gegevens te verstrekken heeft geen invloed op het tot stand komen van de werkovereenkomst.

Bij een betaald dienstverband worden gegevens gevraagd die wettelijk verplicht zijn en die te maken hebben met de salarisadministratie en de Arbodienst.

De (soort) verzamelde gegevens

Voorop staat dat zo min mogelijk gegevens worden verzameld.

De identificerende gegevens bestaan uit naam, adres, postcode, woonplaats, telefoonnummer en geboortedatum.

De toekomstige medewerker wordt gevraagd een identiteitsbewijs te tonen, zodat de identiteit van de persoon kan worden vastgesteld; van de vaststelling wordt een aantekening gemaakt. Bij onbetaalde werkovereenkomsten wordt het BSN niet genoteerd. Bij een betaald dienstverband wordt het BSN wel genoteerd en een kopie van het identiteitsbewijs gemaakt.

Ook wordt gevraagd om een contactpersoon en telefoonnummer in geval van nood. Het geven van deze informatie mag geweigerd worden.

De toekomstige medewerker wordt gevraagd of hij, in het kader van zijn/haar eigen veiligheid en welzijn op de werkvloer, op vrijwillige basis informatie wil geven die leidinggevend kunnen helpen. Voorbeelden zijn het hebben van diabetes (hoe te reageren bij onwel worden), een pacemaker (geen gebruik AED), een rughernia of paniekaanvallen.

In geval van een betaald dienstverband worden tevens gegevens gevraagd die noodzakelijk zijn voor een correcte salarisadministratie.

De medewerker heeft het recht op inzage in zijn/haar gegevens en heeft toegang tot het eigen personeelsdossier.

Toestemming

Voor iedereen die bij Het Warenhuis arbeid verricht wordt een intakeformulier ingevuld in het bijzijn van de betreffende persoon. Mondeling wordt toegelicht dat de informatie vrijwillig wordt verstrekt zodat er werkelijk sprake is van een weloverwogen toestemming (informed consent).

Gegevensbeveiliging

Het Warenhuis spant zich in om de veiligheid van gegevens te waarborgen. De uitgangspunten hierbij zijn:

Beperking van het aantal mensen met toegang tot persoonsgegevens

Binnen Het Warenhuis zijn de verwerkers de directeur van Het Warenhuis, de HR manager, de operationeel manager, de coördinatoren en de meewerkend voormensen.

Deze mensen hebben een geheimhoudingsverklaring ondertekend en een Verklaring omtrent Gedrag verkregen.

Gegevens worden echter ook extern opgeslagen bij de volgende organisaties:

- BDO. Het betreft alleen personen die een betaald dienstverband hebben bij Het Warenhuis. Het doel is salarisverwerking.
- BrinQer. Het betreft alleen personen die een betaald dienstverband hebben. Het doel is verzuimbeheer.

Met deze organisaties is een verwerkersovereenkomst afgesloten.

Beveiliging van documenten (papier en digitaal)

De verwerkers binnen Het Warenhuis hebben allen een wachtwoord voor hun gebruikersprofiel op de computer.

Alleen van werknemers (betaald in dienst) bestaat nog een papieren dossier. Papieren dossiers zitten in een dossierkast die afgesloten is, tenzij er informatie in- of uitgehaald wordt.

De verwerkers hanteren een clean desk policy.

Datalekken

Na het constateren van een datalek zal elke actie ondernomen worden die nodig is om het lek te dichten. Welke actie wordt ondernomen is afhankelijk van het soort lek.

Binnen 72 uur zal het voorval gemeld worden aan de Autoriteit Persoonsgegevens en aan alle (mogelijke) slachtoffers.

Bewaartermijnen

Er worden verschillende termijnen gehanteerd.

Vijf jaar

Gegevens van medewerkers met een betaald dienstverband worden tot vijf jaar na het jaar waarin de werkovereenkomst wordt beëindigd bewaard. Verwijdering van gegevens gebeurt eenmaal per kalenderjaar.

Twee jaar

Gegevens van overige medewerkers worden tot twee jaar na het jaar waarin de werkovereenkomst wordt beëindigd bewaard. Verwijdering van gegevens gebeurt eenmaal per kalenderjaar.

Gegevens worden bewaard om bij een eventuele terugkeer naar Het Warenhuis snel de inschrijving te kunnen hernieuwen en ook de geschiedenis van de medewerker weer te kunnen terugroepen.

Voor de termijn van twee jaar is gekozen omdat de meeste mensen die uitstromen en terugkeren dat doen binnen deze termijn. Dit heeft te maken met de beperkte duur van werkgerelateerde trajecten. Na het uitstromen is daarom binnen twee jaar duidelijk of de uitstroom succesvol is of niet en of terugkeer naar Het Warenhuis gewenst is.

DEEL 2: KLANTEN

Het doel van gegevensverzameling

De enige reden waarom klantgegevens worden verzameld is om het ophalen en/of bezorgen van goederen of het uitlenen van een aanhangwagen mogelijk te maken.

De gegevens worden niet aan derden verstrekt en niet gebruikt voor promotiedoeleinden.

De (soort) verzamelde gegevens

Bij het maken van een ophaal- of bezorgafpraak wordt de klant gevraagd naam, adres, postcode, woonplaats en telefoonnummer te verstrekken. Bij het lenen van een aanhangwagen wordt in aanvulling daarop gevraagd naar een e-mailadres, IBAN en kenteken van de trekkende auto.

Toestemming

Zonder de verstrekking van deze gegevens is de dienstverlening niet mogelijk. Op verschillende pagina's van de website www.kringloopwarenhuis.nl wordt de klant op de hoogte gebracht van het verzamelen en bewaren van persoonsgegevens.

Gegevensbeveiliging

Het Warenhuis spant zich in om de veiligheid van gegevens te waarborgen. De uitgangspunten hierbij zijn:

Beperking van het aantal mensen met toegang tot persoonsgegevens

Binnen Het Warenhuis hebben alleen de medewerkers van het telefoonteam, kassamedewerkers, coördinatoren, de directeur en de operationeel manager via een wachtwoord toegang tot de klantgegevens.

De klantgegevens worden bij twee externe partijen ondergebracht via het kassasysteem en de afsprakensoftware. Met deze partijen is een verwerkersovereenkomst gesloten.

Beveiliging van documenten (papier en digitaal)

Elke kassamedewerker heeft een eigen wachtwoord en bij het Telefoonteam heeft elk profiel een wachtwoord.

Datalekken

Na het constateren van een datalek zal elke actie ondernomen worden die nodig is om het lek te dichten. Welke actie wordt ondernomen is afhankelijk van het soort lek.

Binnen 72 uur zal het voorval gemeld worden aan de Autoriteit Persoonsgegevens en aan alle (mogelijke) slachtoffers.

Bewaartermijn

Klantgegevens worden eenmaal per kalenderjaar gewist/weggegooid.

DEEL 3: GEREGISTREERDE PERSONEN IN HET KADER VAN DE UITVOERING VAN HET GEMEENTELIJKE FIETS FOUT = FIETS WEG BELEID

Het doel van gegevensverzameling

Het doel van de gegevensverzameling is het voldoen aan de contractuele verplichtingen in het kader van het gemeentelijke Fiets Fout = Fiets Weg-beleid tussen Het Warenhuis en de gemeente Leiden.

De (soort) verzamelde gegevens

De verzamelde gegevens zijn wettelijk bepaald. De gegevens worden online opgeslagen in een door de gemeente Leiden beheerde omgeving.

Toestemming

Het verstrekken van de gegevens wordt gedaan in het kader van het voldoen aan een wettelijke verplichting en is noodzakelijk voor het terugkrijgen van de fiets.

Gegevensbeveiliging

Het Warenhuis spant zich in om de veiligheid van gegevens te waarborgen. De uitgangspunten hierbij zijn:

Beperking van het aantal mensen met toegang tot persoonsgegevens

Alleen medewerkers met toestemming hebben toegang tot de gegevens.

Beveiliging van documenten

Alle medewerkers die toestemming hebben om de gegevens te verzamelen hebben een persoonlijke toegangscode. Ten behoeve van de klant wordt er één document geprint en aan de klant verstrekt. Het Warenhuis bewaart geen papieren documenten bij de uitvoering van het Fiets Fout = Fiets Weg-beleid.

Datalekken

Na het constateren van een datalek zal elke actie ondernomen worden die nodig is om het lek te dichten. Welke actie wordt ondernomen is afhankelijk van het soort lek.

Direct na ontdekking zal contact opgenomen worden met de gemeente Leiden en binnen 72 uur zal melding gedaan worden bij de Autoriteit Persoonsgegevens.

Bewaartermijn

Processen-verbaal staan digitaal in het systeem van de gemeente. De gemeente is verantwoordelijk voor bewaren, beveiligen en vernietigen.