# OMNEXT PRIVACY POLICY

## Table of contents

# 1 DEFINITIES

- De **betrokkene** (data subject) = persoon over wie de persoonsgegevens informatie bevatten.
- De **verwerkingsverantwoordelijke** (controller) = degene die doel en middelen van de verwerking bepaalt.
- De **verwerker** (processor) = partij die (als leverancier) persoonsgegevens verwerkt in opdracht en ten behoeve van de verwerkingsverantwoordelijke (diens klant).
- De **Autoriteit persoonsgegevens** (AP) = de Nederlandse toezichthouder die de AVG handhaaft. Taken van de AP zijn onder meer: toezicht, advisering, voorlichting en internationale taken.
- De **Functionaris voor de gegevensbescherming** (DPO) = interne toezichthouder.
- **Verwerkersovereenkomst:** als een verwerkingsverantwoordelijke een verwerker inschakelt, moeten partijen bepaalde afspraken maken met elkaar over de verwerking. Deze afspraken over de verwerking van persoonsgegevens kunnen worden uitgewerkt in een verwerkersovereenkomst.
- **Beveiliging ('technische en organisatorische maatregelen')**: nieuw in de AVG is dat de verwerker naast de verwerkingsverantwoordelijke ook een zelfstandige plicht heeft om 'passende technische en organisatorische maatregelen' te treffen om een 'op het risico afgestemd beveiligingsniveau te waarborgen'. Daarbij kan bijvoorbeeld worden gedacht aan: pseudonimisering en versleuteling, het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen en het vermogen om bij een incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen (back-ups, redundantie).
- **Registerplicht:** zowel de verwerker als de verwerkingsverantwoordelijke moeten een register bijhouden van alle verwerkingsactiviteiten.

Een paar begrippen die vooral van belang zijn voor de verwerkingsverantwoordelijke:

- **Doel**: persoonsgegevens mogen alleen voor, door de verwerkingsverantwoordelijke welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. Vervolgens mogen de persoonsgegevens alleen verder worden verwerkt voor doeleinden die met dat vooraf omschreven doel verenigbaar zijn.
- **Grondslag**: de verwerkingsverantwoordelijke mag alleen gegevens verwerken als hij daarvoor *grondslag* heeft. De grondslagen worden genoemd in artikel 6 AVG (voor 'gewone' persoonsgegevens), artikel 9 AVG (voor bijzondere persoonsgegevens) en artikel 10 AVG (strafrechtelijke gegevens). In artikel 7 en 8 AVG worden nadere eisen gesteld aan de grondslag 'toestemming'.
- **Transparantie**: de verwerkingsverantwoordelijke heeft de plicht de betrokkene te informeren.
- **Rechten betrokkene**: de verwerkingsverantwoordelijke moet de rechten van betrokkenen, zoals recht op inzage, recht op verbetering en recht op dataportabiliteit respecteren.
- **Melden inbreuk in verband met persoonsgegevens (datalek)**: het is de taak van de verwerkingsverantwoordelijke om alle datelekken te documenteren en bepaalde datalekken te melden aan de AP en/of betrokkenen.
- **Privacy impact assessment**: een data Privacy Impact Assessment (PIA) is een verplicht instrument om vooraf na te denken over de privacy-risico's van een bepaalde gegevensverwerking en deze risico's vervolgens te verkleinen door aanpassingen te doen.

# 2 REGISTER VAN VERWERKINGEN

## 2.1 Data

| Data | Omschrijving | Doel verwerking |
|---|---|---|
| HR data | Personeelsdossiers | Beheren personeelsdossiers per medewerker |
| Financiële data | Salarisgegevens | Beheren salarisgegevens per medewerker |
| Klant data | CRM gegevens | Beheren accountinformatie per klant/prospect |
| Account data | Toegang software analyse portalen | Toegang geven tot resultaten software analyses in een webportaal. User Id's kunnen zakelijke e-mailadressen zijn. |

**HR Data:** deze gegevens zijn noodzakelijk voor het administreren van personeelsinformatie. Zo dient de identiteit te worden gecontroleerd en zijn er meerdere gegevens vereist voordat iemand in dienst kan komen. Daarnaast is er een verplichting toe naar de Belastingdienst.

**Financiële data:** deze gegevens zijn noodzakelijk voor de loonadministratie. Zo dient er bijvoorbeeld een loonheffingsformulier aanwezig te zijn en zijn er meerdere gegevens vereist voordat er salaris betaald kan worden. Daarnaast is er een verplichting toe naar de Belastingdienst.

**Klantdata:** deze gegevens zijn noodzakelijk om bijvoorbeeld te kunnen corresponderen met klanten.

**Accountdata:** deze gegevens zijn noodzakelijk om toegang te geven tot de resultaten van de software analyses, welke in een webportaal inzichtelijk zijn. Daarnaast worden loginpogingen met behulp van het account gelogd, welke noodzakelijk zijn voor security audit doeleinden. De accountdata wordt verwijderd op het moment een gebruiker geen toegang meer heeft tot de software analyse resultaten.

Deze gegevens worden slechts verstrekt aan de hieronder genoemde functies.

| Data | Doel verwerking | Betrokkenen |
|---|---|---|
| HR data | Personeelsdossiers | Office manager<br>Directie<br>Microsoft |
| Financiële data | Salarisgegevens | Office manager<br>Directie<br>4-Vision<br>Vitacon |
| Klantdata | CRM gegevens | Office manager<br>Directie<br>Sales<br>Consultants<br>Microsoft |
| Account data | Toegang software analyse portalen | Consultants |

## 2.2 Doelomschrijving, rechtsgrond en onderbouwing verzamelen persoonsgegevens

De betrokkene is verplicht om de gevraagde persoonsgegevens te verstrekken. Wanneer de persoonsgegevens niet verstrekt worden, kan iemand niet in dienst komen of kan er niet gecorrespondeerd worden met potentiële klanten. De betrokkene kan vragen om inzage, rectificatie of het wissen van persoonsgegevens, een klacht indienen of bezwaar maken bij de betreffende verwerkers. Dit kan schriftelijk aangegeven worden via het e-mailadres van de verwerkingsverantwoordelijke. Wanneer het niet meer noodzakelijk is de gegevens te bewaren, zullen deze verwijderd worden.

## 2.3 Bewaartermijnen persoonsgegevens

**HR data**: de loonbelastingverklaring en het ID-bewijs wordt minimaal 7 jaar bewaard. Met betrekking tot sollicitaties en recruitment worden de gegevens tot uiterlijk vier weken na afloop van de sollicitatieprocedure bewaard. Als wij in de toekomst opnieuw contact met de sollicitant willen opnemen, dan vragen wij toestemming om de persoonsgegevens langer op te mogen slaan. Dat zal dan maximaal één jaar zijn.

**Financiële data**: de loonadministratie wordt 7 jaar bewaard.

**Klantdata**: deze data wordt 7 jaar bewaard, tenzij de gegevens niet meer actueel zijn. Er vindt een jaarlijkse opschoonronde plaats om te bepalen of gegevens verwijderd of aangepast dienen te worden.

**Accountdata:** deze data wordt bewaard zolang een gebruiker toegang heeft tot de Omnext software analysediensten.

# 3 FUNCTIONARIS VOOR DE GEGEVENSBESCHERMING/PRIVACY OFFICER

De rol van Privacy Officer is gekoppeld aan de rol van de Security Officer binnen Omnext. De Security/Privacy Officer is de eerste contactpersoon binnen Omnext ten aanzien van privacy/gegevensbescherming gerelateerde zaken.

# 4 VERWERKERSOVEREENKOMST

Binnen de processen van Omnext waar privacy gevoelige informatie verwerkt wordt, is er sprake van een aantal verwerkers.

- Microsoft
- 4-Vision
- Vitaconline

Met beide partijen is een verwerkersovereenkomst afgesloten. In het geval van Microsoft is de verwerkersovereenkomst onderdeel van de algemene voorwaarden (zie http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31). Beide documenten zijn als separaat document beschikbaar.

# 5 PROCEDURE MELDEN DATALEKKEN

## 5.1 Stap 0: definities datalekken

De volgende definities zijn gebaseerd op de richtsnoeren meldplicht datalekken van de Autoriteit Persoonsgegevens. Het securityteam kent de volgende definities en past deze toe.

- Een **incident** is een concrete gebeurtenis waarbij de beschikbaarheid, confidentialiteit of integriteit van een informatie-asset is geschonden. Niet elk incident is een datalek. Het is wel verstandig elk incident te loggen en te analyseren.
- Een **datalek** is een incident waarbij er persoonsgegevens verloren zijn gegaan of als er onrechtmatige verwerking heeft plaatsgevonden.
- Een **persoonsgegeven** is elk gegeven dat herleidbaar is tot een natuurlijk persoon. Denk aan email, telefoonnummer, voornaam_achternaam, huisadres, kenteken, IP-nummer, bankrekeningnummer, MAC-adres, foto's met gezichten erop, inkomen, geboortedatum. Niet persoongegevens zijn gemiddeldes over grotere groepen.

Elk beveiligingsincident wordt gemeld bij de security/privacy officer en wordt gelogd en geanalyseerd. Op basis van het geregistreerde incident wordt bepaald of er sprake is van een datalek.

## 5.2 Stap 1: Melden van datalekken aan Security Officer

Iedereen bij Omnext die werkt met persoonsgegevens, is op de hoogte van het feit dat er een meldplicht datalekken is en dat zij een incident of datalek direct moeten melden. Omnext heeft een Security Officer en incidenten kunnen geregistreerd worden via een aparte site op het Omnext intranet. Deze informatie is opgenomen in security-trainingen en in het personeelsreglement zodat iedereen weet hoe te melden.

## 5.3 Stap 2: vastleggen en analyseren

**Vastleggen en uitzoeken**: De medewerker logt het incident en de Security Officer analyseert het incident, zoekt uit wat er wanneer en waar is gebeurd en welke apparatuur en partijen hierbij betrokken zijn geweest.
**Directe actie**: Indien nodig wordt er directe actie ondernomen om het lek te dichten of te stoppen. Denk aan uitzetten servers, blokkeren accounts of verwijderen van gevoelige data.
**Besluit persoonsgegevens**: Er wordt bepaald welke persoonsgegevens van hoeveel en welke personen er betrokken zijn. Als uitkomst hiervan wordt het aantal personen vastgelegd, welke soorten gegevens en of er sprake is van bijzondere gegevens.
Bepaal de **verantwoordelijke**: Er wordt bepaald wie de verantwoordelijke voor de gegevens is. Dit wordt bepaald door na te gaan hoe de gegevens zijn verkregen en door bestudering van alle bewerkers-overeenkomsten waaronder de gegevens zijn doorgegeven. De verantwoordelijk kan een klant zijn, of de organisatie zelf.
Bepaal **uitsluitbaarheid**: Soms is het redelijkerwijs uit te sluiten dat persoonsgegevens onrechtmatig zijn verwerkt. Dit is bijvoorbeeld het geval bij diefstal van een laptop die voorzien is van sterke encryptie. Goede encryptie leidt tot uitsluitbaarheid. Zonder goede encryptie is er geen uitsluitbaarheid.

## 5.4 Stap 3a: Melden als bewerker/verwerker

Als Omnext zelf niet de verantwoordelijke is, wordt er melding gedaan conform de contactgegevens in verwerkersovereenkomst. Indien dit niet duidelijk is of niet uitvoerbaar, wordt contact opgenomen via telefoonnummer op website van partij. Het streven is om dit te doen binnen 8 kantooruren na ontdekking incident (of conform termijn in verwerkersovereenkomst). De verantwoordelijke moet zorgen voor de overige meldingen. De organisatie volgt verder alleen de instructies van de verantwoordelijke.

## 5.5 Stap 3b: Melden als verantwoordelijke

Als er sprake is van een niet uitsluitbaar datalek en Omnext de verantwoordelijke partij is, dan worden de volgende stappen ondernomen:

- Op de hoogte brengen van de directie, zodat zij kunnen meedenken over communicatie.
- Afronden onderzoek en vastleggen uitkomsten in een apart incidentrapport
- Inschatten ernst incident: Een incident is ernstig als er sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Een incident met gevoelige persoonsgegevens is altijd ernstig, ook met 1 persoon. Een incident zonder gevoelige persoonsgegevens is ernstig bij een voldoende omvang.
- Als het datalek ernstig is, dan wordt het incident via het webformulier: https://datalekken.autoriteitpersoonsgegevens.nl/melding/ gemeld bij de Autoriteit Persoonsgegevens. Dit gebeurt indien mogelijk binnen 72 uur na ontdekking.
- Er wordt ingeschat of het melden aan betrokkenen mogelijk is en of een melding eventueel nadelige gevolgen heeft voor de betrokken persoon. Als het mogelijk is om te melden, dit geen nadelen heeft voor betrokkenen en er geen sprake is van goede encryptie, worden het datalek gemeld aan betrokkenen.
- Er wordt een verbeterplan gemaakt die toekomstige datalekken kunnen voorkomen.

## 5.6 Stap 4: Periodieke review

De gegevens van het incident, alle besluiten en de melding worden bewaard als onderdeel van het ISMS door het information securityteam. Meldingen worden minimaal een jaar bewaard vanuit de wet bescherming persoonsgegevens. Elk half jaar worden alle incidenten van de afgelopen periode nogmaals bestudeerd. Er wordt dan opnieuw gekeken met eventuele nieuwe informatie of er alsnog gemeld moet worden. Als dat zo is, wordt er alsnog gemeld.

## 5.7 Stap 5: Voorbereid zijn op datalekken

De volgende stappen zijn genomen om het risico van datalekken te verkleinen:

- De processen waarin persoonsgegevens worden gebruikt zijn in kaart gebracht. Per proces is uitgezocht om wat voor persoonsgegevens het gaat.
- Er is een bewerkersovereenkomst met elke klant en leverancier waarmee persoonsgegevens worden gedeeld. Zodat er duidelijkheid is over wie er gemeld moet worden.
- Er is gezorgd voor een goede beveiliging van de organisatie door middel van het opzetten van een Informatiebeveiligingsbeleid.
- Regelmatig wordt er een security awareness training gegeven waarbij iedereen goed op de hoogte wordt gebracht van het belang van beveiliging.

# 6 INFORMATIEBEVEILIGINGSBELEID

Omnext heeft het informatiebeveiligingsbeleid beschreven in een aantal beleidsdocumenten, die toegankelijk zijn voor alle betrokken medewerkers. Het informatiebeveiligingsproces is beoordeeld en gecertificeerd op basis van ISO 27001 door een externe partij.

# 7 PRIVACY IMPACT ANALYSE BESCHIKBAAR

Er is een Privacy Impact Analyse (PIA) uitgevoerd binnen Omnext die beschikbaar is als separaat document.