Ministerie van Justitie en Veiligheid

Factsheet

Verwerkersovereenkomst

Schept duidelijkheid over privacybescherming bij online diensten

De vraag

In de afgelopen jaren zijn veel organisaties binnen de Rijksoverheid zich aan het oriënteren op de mogelijkheid om Microsoft-clouddiensten af te nemen. Hoe zijn de rechten en plichten van Microsoft vastgelegd met betrekking tot privacybescherming en naleving van de Algemene Verordening Gegevensbescherming (AVG) voor deze online producten en diensten?

De oplossing

De verwerkersovereenkomst tussen de Rijksoverheid en Microsoft bindt Microsoft aan instructies voor de verwerking van persoonsgegevens van de (werknemers van) overheidsorganisaties. Deze afspraken beschrijven wat Microsoft wel, en wat Microsoft niet met deze gegevens mag doen. De verwerkersovereenkomst komt voort uit de expertise van Strategisch Leveranciersmanagement Microsoft Rijk (SLM) en gebaseerd op nauw overleg tussen SLM en Microsoft. De verwerkersovereenkomst voldoet niet alleen aan de eisen van de AVG, het gaat in sommige opzichten verder dan de AVG en biedt zodoende meer bescherming.
De verwerkersovereenkomst tussen de Rijksoverheid en Microsoft beschrijft onder meer afspraken over:

1. Het doel van de verwerking

Microsoft mag de persoonsgegevens van de (werknemers van) overheidsorganisaties enkel en alleen verwerken voor gespecificeerde, door de Rijksoverheid toegestane doeleinden. In de verwerkersovereenkomst staan deze als volgt beschreven:

(a) Uitvoeren (het leveren en verbeteren van de Online Diensten, identificeren en mitigeren van afwijkingen, “bugs”, en andere problemen met Online Diensten door middel van het leveren van aanpassingen van de Online Diensten).
(b) Onverminderd (a) hierboven, Beveiliging (identificeren en mitigeren van beveiligingsdreigingen en risico’s).
(c) Onverminderd (a) hierboven, Actueel (leveren en installeren van de laatste updates van de Online Diensten).

De Rijksoverheid heeft ook doeleinden benoemd waarvoor Microsoft expliciet géén goedkeuring wordt gegeven, namelijk:

(a) data analytics,
(b) profilering (inclusief, maar niet beperkt tot het creëren van psychometrische, psychografische of andere gebruikersprofielen),
(c) adverteren (inclusief gerichte aanbevelingen op het scherm voor producten of diensten, aangeboden door Microsoft, maar niet gelicentieerd of gebruikt door de Klant) of een vergelijkbaar commercieel doel, of
(d) marktonderzoek gericht op het creëren van nieuwe functionaliteiten, diensten of producten of enig ander doel;

tenzij dit is toegestaan op basis van schriftelijke instructies van de Rijksoverheid. Dat is bijzonder omdat de doelen zo nauwkeurig zijn afgebakend en omdat de Rijksoverheid een verbodsinstructie geeft.
Het bovenstaande weerhoudt Microsoft er niet van om gegevens te verwerken voor de legitieme bedrijfsvoering. Ook daarvoor benoemt de verwerkersovereenkomst expliciet de activiteiten die toegestaan zijn. Hiertoe behoren onder meer facturatie, account management en het bestrijden van fraude en cybercriminaliteit.

2. Anonimiseren

Microsoft zal de gegevens bovendien anonimiseren volgens de richtlijnen van de privacytoezichthouders uit 2014 (WP216).

3. Afspraken over sub-processors

Microsoft kan een deel van de verwerkingsactiviteiten uitbesteden aan een onderaannemer (een sub-processor). Microsoft dient ervoor te zorgen dat sub-processors werken binnen de bandbreedte van Microsofts eigen instructie over hun plichten ten aanzien van privacybescherming. SLM controleert periodiek de afspraken die Microsoft met zijn onderaannemers maakt om naleving van de afspraken te garanderen.

4. Recht om audits uit te voeren

De Rijksoverheid heeft het recht om periodiek te controleren of dit in de praktijk ook het geval is. Deze audits vinden jaarlijks plaats. Het audit recht is een sterk middel om naleving af te dwingen en te garanderen. SLM publiceert vervolgens een samenvatting van de bevindingen op zijn website.

De meerwaarde van de afspraken

Door de contractonderhandelingen tussen SLM en Microsoft zijn de persoonsgegevens van de werknemers van de instanties die onder de verwerkersovereenkomst vallen beter beschermd.

Aansluiten bij de Microsoft Business Services Agreement (MBSA)?

De reikwijdte van de verwerkersovereenkomst strekt zich uit tot de Rijksdiensten en de daarbij behorende ZBO's en Agentschappen die aangesloten zijn bij de rijksbrede Microsoft Business en Services Agreement (MBSA) die beheerd wordt door SLM.

Deze organisaties hoeven niet zelf actie te ondernemen om de afspraken van Microsoft van toepassing te laten zijn op hun contracten met de leverancier.

Wilt u meer informatie over de verwerkersovereenkomst of wilt u zich aansluiten bij de MBSA?
Neem dan contact op via SLMMicrosoft@minjev.nl of kijk op www.slmmicrosoftrijk.nl.

Over de verwerkersovereenkomst

Een verwerkingsovereenkomst geeft invulling aan de verplichting die Artikel 28 lid 3 van de AVG stelt ten aanzien van de verwerking van persoonsgegevens: De verwerking door een verwerker wordt geregeld in een overeenkomst of andere rechtshandeling krachtens het Unierecht of het lidstatelijke recht dat de verwerker ten aanzien van de verwerkingsverantwoordelijke bindt, en waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de verwerkingsverantwoordelijke worden omschreven.

Concreet betekent dit dat iedere organisatie die persoonsgegevens verwerkt zich aan de privacywetgeving moet houden. De AVG geeft een duidelijke taakverdeling aan tussen de gegevensverantwoordelijke (data controller) en de gegevensverwerker (data processor). Dit zijn de twee partijen die de verwerkersovereenkomst aangaan. Elk van deze rollen kent zijn eigen verplichtingen en beperkingen ten aanzien van gegevensverwerking.