DE AVG, WAT NU?

André Kamps en
Jan Pieter Schuitema

Jan Pieter Schuitema

NAAM
André Kamps en
Jan Pieter Schuitema

WERKZAAM BIJ
De IT-jurist

WEBSITE
www.it-jurist.nl

Het is bijna 25 mei 2018, de dag waarop de Algemene Verordening Gegevensbescherming (AVG) van toepassing wordt. In vorige edities van dit magazine zijn al verschillende belangrijke onderwerpen uit die AVG behandeld. Deze keer een praktisch vervolgartikel over wat de AVG nu concreet voor het mkb-accountantskantoor betekent.

De eerste vraag die natuurlijk gesteld moet worden is of de AVG wel van toepassing is op de mkb-accountant. Het antwoord kan bijna niet anders zijn dan ja. Dat het mkb-accountantskantoor géén persoonsgegevens verwerkt, lijkt welhaast ondenkbaar. Denk bijvoorbeeld maar eens aan de salarisadministratie of de fiscale aangifte. En wanneer er persoonsgegevens verwerkt worden, is de AVG op de mkb-accountantspraktijk van toepassing.

UITGANGSPUNT: HET VERWERKINGSREGISTER

Voor de mkb-accountant is het allereerst goed om in beeld te krijgen welke diensten hij verleent en vooral welke persoonsgegevens hij daarbij verwerkt. Daarbij is het ook van belang om de daarbij gebruikte applicaties en eventuele verwerkers in beeld te brengen. Ook het helder krijgen wie toegang heeft tot verwerkte persoonsgegevens is belangrijk. Wanneer de mkb-accountant deze informatie verwerkt in een overzichtelijk register (bijvoorbeeld een Excel-bestand) dan is dat niet alleen handig en praktisch voor het overzicht van de accountant zelf, maar voldoet hij ook meteen, indien van toepassing, aan de verplichting tot het hebben van een verwerkingsregister. Het register is verplicht voor organisaties met meer dan 250 medewerkers, maar ook voor kleinere organisaties, wanneer het waarschijnlijk is dat de verwerking een risico inhoudt voor de rechten van betrokkenen, de verwerking niet incidenteel is of de verwerking bijzondere persoonsgegevens verwerkt. Het is dus altijd zinvol om een dergelijk register bij te houden, ook als dat niet verplicht is. Let daarbij wel op dat de mkb-accountant twee verschillende rollen kan spelen, verwerkingsverantwoordelijke en in sommige gevallen verwerker. Voor beide rollen moet een apart register worden opgesteld. Met de zojuist genoemde onderwerpen is het verwerkingsregister overigens nog niet compleet. Vermeld in het register ook uw contactgegevens, de verwerkingsdoeleinden en eventueel de grondslag(en), bewaartermijnen en indien mogelijk de getroffen beveiligingsmaatregelen.

PRIVACY BY DESIGN & PRIVACY BY DEFAULT

Nadat het kantoor inzichtelijk heeft gemaakt hoe de gegevensverwerkingsproces eruit ziet, is het aan de mkb-accountant en de organisatie om ervoor te zorgen dat dit proces voldoet aan de in de AVG genoemde uitgangspunten. Een nieuw uitgangspunt voor gegevensverwerking dat uit de AVG voortvloeit is privacy by design (door ontwerp) en privacy by default (door standaardinstellingen). De mkb-accountant dient als verwerkingsverantwoordelijke (en ook als verwerker) bij het verwerkingsproces van persoonsgegevens rekening te houden met deze principes. Privacy by design houdt in dat de mkb-accountant bij het ontwerpen van diensten en producten zo veel mogelijk rekening houdt met gegevensbescherming en privacy. Hieronder valt onder meer het beschermen van persoonsgegevens door bijvoorbeeld pseudonimisering en anonimisering en een adequate beveiliging.
Voor de mkb-accountant is pseudonimisering een mogelijke maatregel om persoonsgegevens te beschermen. Dit kan bijvoorbeeld eenvoudig door (klant)namen te vervangen door nummers. Ook data-minimalisatie is een belangrijk onderdeel van privacy by design. Het verwerken van persoonsgegevens beperken tot hetgeen strikt noodzakelijk is voor het doel van de verwerking, is een belangrijke maatregel die de mkb-accountant moet nemen. Het bewaren van een kopie van een legitimatiebewijs in het kader van de Wwft is bijvoorbeeld iets wat niet strikt noodzakelijk is maar wat toch nog vaak gedaan wordt. Ondanks dat het nog is toegestaan, kan de vraag worden gesteld of dat nog steeds verantwoord is gelet op de beginselen van de AVG, zoals dataminimalisatie. Privacy by default houdt in dat er maatregelen moeten worden getroffen, dat er alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor een specifiek doel. >

“EEN BELANGRIJKE PLICHT VOOR DE MKB-ACCOUNTANT IS HET TREFFEN VAN PASSENDE TECHNISCHE EN ORGANISATORISCHE MAATREGELEN TER BEVEILIGING VAN DE PERSOONSGEGEVENS.”

André Kamps

Een voorbeeld is dat wanneer een klant zich wil inschrijven op een nieuwsbrief van een accountantskantoor, dat er niet onnodig veel gegevens worden gevraagd. Een naam en e-mailadres is in dat geval al voldoende.

BEVEILIGINGSMAATREGELEN

Een belangrijke plicht voor de mkb-accountant is het treffen van passende technische en organisatorische maatregelen ter beveiliging van de persoonsgegevens. De beveiliging moet een beveiligingsniveau waarborgen dat is afgestemd op het risico dat de verwerking van persoonsgegevens door de accountant met zich kan meebrengen. Bij het vaststellen van de juiste beveiligingsmaatregelen moet u eerst het risico objectief vaststellen.

Daarna kunt u afwegen welke beveiligingsmaatregelen daarbij passend zijn. Dit betekent dat de maatregelen die u neemt in verhouding staan tot de gegevens en de eventuele risico's van de verwerking. Het is dus niet altijd nodig om de zwaarst mogelijk maatregelen te nemen. Hoe groter het risico, hoe zwaarder de maatregelen die u moet treffen. Bij het bepalen van de passende maatregelen moet u ook onder meer rekening houden met de uitvoeringskosten, de stand van de techniek, de omvang van de verwerking en de waarschijnlijkheid dat de eerder vastgestelde risico's zich zullen verwezenlijken. Zorg ook dat de beveiligingsmaatregelen die u treft actueel en passend blijven. Leg daarnaast de eisen aan de beveiliging van persoonsgegevens ook op aan eventuele (sub-) verwerkers.

DATALEKKEN

De omgang met inbreuken in verband met persoonsgegevens, oftewel datalekken, is niet geheel nieuw. De praktijk heeft al kennis kunnen maken met de meldplicht via de Meldplicht datalekken die in de Wet bescherming persoonsgegevens is opgenomen sinds 2016. De meldplicht in de AVG is iets anders vormgegeven. Een datalek moet altijd aan de Autoriteit Persoonsgegevens (AP) gemeld worden, tenzij het niet waarschijnlijk is dat het datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. De melding moet, indien mogelijk, uiterlijk binnen 72 uur plaatsvinden nadat de verwerkingsverantwoordelijke van het datalek kennis heeft genomen. Een melding aan een betrokkene moet volgens de AVG onverwijld plaatsvinden als het datalek een waarschijnlijk hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Uitzonderingen hierop zijn die gevallen waarin de gegevens zijn versleuteld of anderszins onbegrijpelijk zijn gemaakt, er maatregelen zijn genomen waardoor het hoge risico voor betrokkenen is verdwenen, het lek een groot aantal gevallen betreft en het zoveel moeite kost dat een openbare mededeling volstaat, of wanneer de melding afbreuk zou doen aan een zwaarwegend belang.

Nieuw is dat de mkb-accountant ieder datalek moet documenteren, of dit nu een datalek is dat gemeld moet worden of niet. Daarbij moeten de feiten en de gevolgen van het datalek en de genomen corrigerende maatregelen worden genoteerd. Omdat de AP om inzage in het document kan vragen moet het document wel zo worden opgemaakt dat de AP daadwerkelijk kan controleren of datalekken worden gerapporteerd en hoe daar vervolgens mee is omgegaan. Er worden geen vormvoorschriften voor het register gegeven. Een Excel-bestand of zelfs een tekstdocument zou al voldoende zijn.

RECHTEN VAN BETROKKENEN

Met de komst van de AVG is het aantal rechten van betrokkenen uitgebreid. Allereerst is het van belang dat bij het verkrijgen van de gegevens de betrokkene wordt geïnformeerd over de gegevensverwerking. De AVG onderscheidt hier twee situaties: gegevens worden rechtstreeks van een betrokkene verkregen of de gegevens worden buiten de betrokkene om verkregen. Voor beide situaties geldt dat wanneer de betrokkene de informatie over de gegevensverwerking al gekregen heeft, de mkb-accountant niet nogmaals die informatie hoeft te verstrekken. Wanneer de mkb-accountant de gegevens via de opdrachtgever ontvangt, is deze opdrachtgever als verwerkingsverantwoordelijke al verplicht om aan de betrokkene te melden dat hij de gegevens doorzendt aan de mkb-accountant. In dat geval hoeft de mkb-accountant dan niet zelf de informatie te verstrekken. Hiervan is sprake wanneer de werkgever gegevens verstrekt van werknemers aan het accountantskantoor. Het opstellen van en het vervolgens verwijzen naar een privacybeleid waarin alle door de AVG verplichte informatie wordt benoemd is tevens nodig.

DATAPORTABILITEIT

Een nieuw recht dat een betrokkene op grond van de AVG krijgt is het recht op dataportabiliteit. Dit houdt in dat de betrokkene de mkb-accountant kan verzoeken om alle persoonsgegevens die hij verwerkt over de betrokkene van de mkb-accountant te ontvangen. Dit recht is toegevoegd aan de AVG, zodat betrokkenen eenvoudiger kunnen overstappen van de ene naar de andere dienstverlener. De vraag kan ook inhouden dat de mkb-accountant de gegevens rechtstreeks overdraagt naar bijvoorbeeld een nieuwe/andere accountant van de betrokkene. De mkb-accountant heeft de plicht om de gegevens in een gestructureerd, veelgebruikt en machineleesbaar formaat te verstrekken. Dit formaat kan een in een bepaalde sector (in dit geval die van de mkb-accountant) gebruikelijk zijn.

VERGETELHEID

Nog een nieuw recht is het zogenaamde recht op vergetelheid. In de Wbp was een vergelijkbaar recht opgenomen maar dat was beperkt tot het verwijderen van onjuiste, onvolledige of niet ter zake doende gegevens. Wanneer een betrokkene erom vraagt, moet de mkb-accountant de betreffende persoonsgegevens wissen. Aan dit recht zit wel een aantal voorwaarden. Zo is het recht op vergetelheid alleen van toepassing als de mkb-accountant de persoonsgegevens niet meer nodig heeft voor de doeleinden waarvoor zij verwerkt zijn. Ook in het geval dat de grondslag voor verwerking toestemming van de betrokkene is en de betrokkene die toestemming intrekt, moeten zijn gegevens verwijderd worden. Andere redenen om voor een mkb-accountant persoonsgegevens op verzoek te moeten verwijderen zijn onrechtmatige verwerking en een wettelijke plicht die de accountant dwingt om de gegevens te wissen. Natuurlijk kan het ook zo zijn dat de mkb-accountant vanwege wet- en regelgeving aan een bewaarplicht moet voldoen en op grond daarvan de gegevens juist niet mag wissen. Andere, al bekende rechten van betrokkenen zijn het recht op inzage, het recht op rectificatie, het recht op beperking van de verwerking, het recht op bezwaar en het recht op een menselijke blik bij besluiten.

"MET DE KOMST VAN DE AVG IS HET AANTAL RECHTEN VAN BETROKKENEN UITGEBREID."

Op welke van deze rechten een betrokkene ook een beroep doet, respecteer dat recht en handel ernaar wanneer het moet. Het opstellen van procedures over de omgang met verzoeken van betrokkenen kan een nuttig hulpmiddel zijn om aan de plichten te voldoen.

UPDATE NOVAK KWALITEITSSYSTEEM

Rond eind maart komt een update beschikbaar voor het Novak Kwaliteitssysteem om de content AVG-compliant te maken. Onderwerpen die in dit artikel zijn beschreven zoals een privacy-beleid, verwerkingsregister, aangescherpte verwerkersovereenkomst, een aanscherping op de instructie persoonsgegevens en de instructie meldplicht datalekken zullen onder andere onderdeel uitmaken van deze update. Door middel van de digitale nieuwsbrief van Novak wordt u op de hoogte gehouden.

Mr. M.H. Kamps en Mr. J.P. Schuitema zijn werkzaam bij het adviesbureau De IT-jurist (www.it-jurist.nl).