Informatiebeveiliging:

Alle SRA-kantoren zijn ermee bezig, niemand is klaar

Een van de grootste risico's voor accountantskantoren en hun mkb-klanten is informatiebeveiliging, zeker nu de Algemene Verordening Gegevensbescherming (AVG) op 25 mei 2018 van kracht wordt en de huidige wet voor bescherming van persoonsgegevens (Wbp) vervangt. Big four-kantoren hebben cybersecurity en privacy vanwege het strategische risico inmiddels hoog op hun beleidsagenda gezet en nemen zelfs IT-bedrijven over. Daarnaast storten allerlei IT-, verzekerings- en adviesbedrijven zich op deze nieuwe markt, want de angst onder mkb-bedrijven is groot. Wat is de status bij SRA-kantoren? "Iedereen is ermee bezig, niemand is klaar", aldus SRA-privacy officer Tony van Oorschot. Hoog tijd voor actie!

Bent u 'in control'?

Heeft u nog nooit een veiligheidsincident gehad of is er geen datalek aan u gerapporteerd? Dan is de kans groot dat u nog niet 'in control' bent want iedereen krijgt er vroeg of laat mee te maken. Weet u bijvoorbeeld waar en wanneer werknemers hun vertrouwelijke bedrijfsdocumenten openen? Hebben uw werknemers nog nooit privacygevoelige gegevens, zoals salarisstroken, naar de verkeerde ontvanger gestuurd of een phishing-mail geopend? En weet u zeker dat uw vertrekkende medewerkers na vertrek niet meer over wachtwoorden kunnen beschikken? Misschien nog wel belangrijker is de vraag of uw medewerkers weten wanneer sprake is van een veiligheidsincident en welke actie ze vervolgens moeten nemen. In bijna de helft van de datalekmeldingen bij de Autoriteit Persoonsgegevens (AP) was slordigheid van de medewerkers de bron. Zorg dus dat u 'in control' komt.

Voorkomen is beter dan genezen

De vraag is vooral: zijn interne procedures voldoende duidelijk als het gaat om bescherming van persoonsgegevens en het melden van datalekken en wie is verantwoordelijk? Controle op data is niet zozeer de verantwoordelijkheid van de IT-afdeling, maar van het gehele accountantskantoor en alle medewerkers. Omdat uw kantoor data verzamelt en verwerkt, bent u verplicht om uw klanten te informeren over wat er met hun gegevens gebeurt en eveneens om datalekken te melden. Wordt er een onderzoek ingesteld, dan moet u bewijzen dat u er alles aan hebt gedaan om het lek te voorkomen. De AP dreigt met boetes die kunnen oplopen tot € 20 miljoen en bij SRA krijgen we vaak de vraag hoe reëel dat risico is. Het antwoord is dat niemand dat precies weet, boetes zijn nog niet uitgedeeld, maar de imagoschade die u zou oplopen bij een datalek, is groot en lastig te genezen! Voorkom dat risico.

Nieuwe procedures

In mei 2016 is de AVG in werking getreden met een overgangsperiode van twee jaar. Op 25 mei 2018 wordt de huidige Wet bescherming persoonsgegevens (Wbp) ingetrokken en definitief vervangen door de AVG. Op deze datum moet u compliant zijn en voldoen aan nieuwe verplichtingen; technisch en organisatorisch. Niet alleen binnen uw organisatie – de interne procedures zoals hierboven beschreven – maar ook richting uw klanten en uw leveranciers. Als controlerend accountant bent u in lijn met Standaard 250 verplicht om de naleving van de AVG te controleren en indien nodig te rapporteren. Als fiscaal adviseur communiceert uw software met de Belastingdienst en met leveranciers. In alle salarissoftware worden privacygevoelige persoonsgegevens verwerkt. Veel kantoren weten niet hoe die processen lopen en welke acties noodzakelijk zijn.

Risico's voor uw klanten

Tot slot zult u zich meer moeten verdiepen in de strategische risico's bij uw klanten. Uit recent onderzoek van de MKB Servicedesk blijkt dat de onwetendheid over de komst van de AVG groot is; de meerderheid van de mkb-ondernemers weet niet eens van het bestaan van de wet, terwijl de consequenties groot zijn en per branche anders kunnen uitpakken. Cameratoezicht bij een sporthal, hotel of winkel moet bijvoorbeeld binnenkort aan strenge regels, zoals een privacytoets, voldoen. In de medische branche is de verwerking van persoonsgegevens aan zeer strenge regels gebonden. De transportbranche werd recent opgeschrikt door een ransome-aanval die de hele Rotterdamse haven heeft platgelegd. Ook voor uw klanten dringt dus de tijd als het gaat om cybersecurity en privacy. Niet langer als een IT-gerelateerd onderwerp, maar als een strategisch risico. Met u als adviseur.

Top 5: wat moet u doen?

1. Creëer intern bewustwording en zorg voor een vast aanspreekpunt
2. Maak een register met persoonsgegevens die u verwerkt
3. Breng risico's in kaart en zorg voor technische (beveiligings-) en organisatorische maatregelen
4. Zorg voor documentatie van datalekken
5. Breng verwerkingen door derden in kaart en sluit bewerkersovereenkomsten

Stappenplan

Om u op weg te helpen, geven we u de belangrijkste handvatten aan de hand van vijf stappen:

1. Bewustwording en een vast aanspreekpunt in uw organisatie

Informeer uw medewerkers over de wetgeving, de impact van de AVG op uw huidige processen en bij wie zij terecht kunnen bij vragen. Onder de AVG krijgen uw klanten meer privacyrechten. Nieuw is bijvoorbeeld de mogelijkheid die klanten hebben om gegevens eenvoudig op te vragen en door te geven aan een andere organisatie.

Tony van Oorschot: "Het is vooral van belang te weten wat er allemaal verstuurd wordt en wat u ontvangt. Stel dat er een veiligheidsincident is: wie is verantwoordelijk, wie bepaalt of het een datalek is, wie gaat het melden? Als je alles onder de wet Wpb op orde had, dan zijn de nieuwe maatregelen beperkt. Zorg dat uw medewerkers zich bewust zijn van de regels en dat ze weten bij wie ze terecht kunnen."

Onder de AVG kunnen organisaties verplicht zijn om een functionaris voor de gegevensverwerking (FG) aan te stellen die toezicht houdt op de toepassing en naleving van de AVG. Deze functionaris heet ook wel: privacy officer, security officer of data protection officer. Uiteraard mag uw organisatie ook vrijwillig een FG aanstellen.

Tony van Oorschot: "Sommige SRA-kantoren hebben deze taak bij de compliance officer belegd. Een enkeling heeft formeel een FG aangesteld. Over het algemeen geldt deze verplichting voor accountantskantoren niet, maar het is raadzaam om iemand verantwoordelijk te maken voor alle werkzaamheden die voortvloeien uit de nieuwe wet. Intern of extern."

Vergeet niet dat ook uw klanten moeten nadenken over het aanstellen van een intern aanspreekpunt, wellicht in de rol van privacy officer. Voor u biedt dat mogelijkheden om deze rol ook richting klanten te vervullen.

2. Registreer waar binnen uw organisatie persoonsgegevens worden verwerkt

Documenteer welke persoonsgegevens u verwerkt en met welk doel, waar deze gegevens vandaan komen en met wie u ze deelt. Belangrijk is de wettelijke grondslag op basis waarvan u de gegevens verwerkt.

Tony van Oorschot: "Alles moet worden bijgehouden in het register: wat doe ik (bijvoorbeeld: loonaangifte), wat (gegevens), voor wie en hoe heb ik dat beveiligd? Belangrijk zijn vooral de rollen en rechten: alleen die personen mogen erin die toestemming hebben. En alleen gegevens van klanten die toestemming hebben gegeven, mogen worden verwerkt."

De AVG stelt strengere eisen aan toestemming. Evalueer daarom de manier waarop u toestemming vraagt, krijgt en registreert. Nieuw is dat u moet kunnen aantonen dat u geldige toestemming van mensen heeft gekregen om hun persoonsgegevens te verwerken. En dat het voor uw klanten net zo makkelijk moet zijn om hun toestemming in te trekken als om die te geven. Omdat voor accountantskantoren veel processen gelijk zijn, maakt SRA voor haar leden een modelregister met veelvoorkomende verwerkingen. U kunt dit model als basis gebruiken voor het opzetten van uw eigen register. Onderdelen zijn:

- De categorieën van betrokkenen en persoonsgegevens
- De doeleinden van verwerking
- De grondslag voor verwerking van gegevens
- De categorieën van ontvangers aan wie de persoonsgegevens worden verstrekt
- Algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen

3. Breng risico's in kaart en zorg voor technische (beveiligings-) en organisatorische maatregelen

Onder de AVG kunt u, of uw klant, verplicht zijn een zogeheten *data protection impact*

assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. U moet een DPIA uitvoeren als uw beoogde gegevensverwerking waarschijnlijk een hoog privacyrisico met zich meebrengt.

Tony van Oorschot: "De DPIA wordt in principe per proces uitgevoerd, maar kan ook voor een organisatie als geheel worden uitgevoerd. Voor veel kantoren zal het uitvoeren van een DPIA niet direct verplicht zijn. Raadzaam is wel om voor de gegevens en verwerkingen in het register de eventuele risico's van de verwerking te classificeren. Op basis hiervan kan vervolgens worden bekeken voor welk(e) proces(sen) een DPIA zinvol is."

Daarnaast zult u 'privacy by design & default' als standaard in de bedrijfsvoering en ICT moeten invoeren. 'Privacy by design' houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat persoonsgegevens goed worden beschermd. 'Privacy by default' houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken. Bijvoorbeeld: als iemand zich op uw nieuwsbrief wil abonneren, mag u niet meer gegevens opvragen dan nodig is.

4. Zorg voor documentatie van datalekken

De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde. De AVG stelt wel strengere eisen aan uw eigen registratie van de datalekken die zich in uw organisatie hebben voorgedaan. U moet alle datalekken documenteren. Met deze documentatie moet de AP kunnen controleren of u aan de meldplicht heeft voldaan. Daarbij gaat het niet alleen om bijhouden van de incidenten waarvoor u een melding heeft gedaan bij de AP maar om alle incidenten, inclusief de afweging die u heeft gemaakt om het incident niet te melden. Gelet op het belang voor de organisatie en de bestuurlijke aansprakelijkheid dient periodiek door de FG te worden gerapporteerd aan de directie en/of het bestuur.

5. Breng verwerkingen door derden in kaart en sluit bewerkersovereenkomsten

Bij verwerking van gegevens is sprake van een verantwoordelijke en een bewerker. De verantwoordelijke bepaalt wat er waarom moet worden verwerkt. De bewerker is de externe partij die dit vervolgens uitvoert, bijvoorbeeld salarisverwerking voor uw klant. Is er gegevensverwerking aan u uitbesteed of heeft u gegevensverwerking uitbesteed aan een (sub)bewerker, bijvoorbeeld een online softwareleverancier? Beoordeel dan of de overeengekomen maatregelen in bestaande contracten met uw bewerkers nog steeds toereikend zijn en voldoen aan de vereisten in de AVG. Zo niet, breng dan tijdig noodzakelijke wijzigingen aan.

Tony van Oorschot: "Neem altijd de drieluik 'klant – interne organisatie – leverancier' als uitgangspunt. Je moet dus richting je klant voldoen aan de regels, maar ook richting leveranciers. Check de contracten en gemaakte afspraken goed voor alle pakketten die zijn uitbesteed en zorg voor bewerkersovereenkomsten. Maakt een dataverwerker een fout, dan bent u aansprakelijk. De belangrijkste vraag bij het uitbesteden van IT is: doet deze dienstverlener er alles aan om een datalek te voorkomen? Controleer goed aan wie u de data toevertrouwt. SRA is bezig met een inventarisatie van leveranciers die aan de regels voldoen."

Zeker richting uw klanten is het raadzaam om de regie te pakken. Niet alleen omdat veel klanten onvoldoende op de hoogte zijn van wat ze moeten doen, maar ook om uw organisatie voor te bereiden en dit proces zo efficiënt mogelijk te laten verlopen.

Tot slot

In het dossier op sra.nl vindt u alle actuele informatie, modellen, een whitepaper, overzicht van bijeenkomsten, relevante informatie en links naar externe bronnen. De tijd dringt, dus als uw organisatie nog niet 'AVG-proof' is, neem dan rechtstreeks contact op voor vragen, advies of begeleiding. U kunt ook via SRA een privacy officer inhuren. Contact: Tony van Oorschot, privacy officer SRA: 030 656 60 60 of tvanoorschot@sra.nl.

TIP

Ga voor een gratis privacyverklaring naar www.veiliginternetten.nl

Ga naar sra.nl voor o.a.:

- SRA-Whitepaper Meldplicht datalekken
- Model Privacyvoorwaarden - inclusief eenzijdige bewerkersovereenkomst (Word)
- Model Bewerkersovereenkomst binnen EU (Word)
- Model Sub Bewerkersovereenkomst binnen EU (Word)
- Model Bewerkersovereenkomst buiten EU - passend beschermingsniveau (Word)
- Model Bewerkersovereenkomst buiten EU - niet passend beschermingsniveau (Word)
- Toelichting op model bewerkersovereenkomst (Word)
- Cursus Privacy Officer in het accountantskantoor (EOCU14195)
- E-learning Privacy en datalekken in het accountantskantoor (ELEC14294)