ST Nieuwsbrief 2018-5

1. Hoe beveilig ik mijn persoonsgegevens?

U moet volgens de AVG uw persoonsgegevens op een juiste en doeltreffende manier beveiligen. Op welke wijze geeft u daar invulling aan?

Zijn er zaken die minimaal geregeld moeten worden? Hoe ga ik met deze verplichting om richting mijn leveranciers en serviceproviders? Want uw onderneming is volgens de AVG verantwoordelijk voor het nemen van passende technische én organisatorische maatregelen om een adequaat beveiligingsniveau te waarborgen voor de verwerking van persoonsgegevens.

Persoonsgegevens goed beveiligen
Hoe moet ik volgens de AVG die persoonsgegevens dan goed beveiligen? Hiervoor moet u met de volgende zaken rekening houden:

- de stand van de techniek – de huidige technische stand van de techniek is voor wat betreft technische maatregelen bepalend voor wat er minimaal van u verwacht wordt
- de aard, de omvang en doeleinden van de verwerkingen – de categorieën van persoonsgegevens in samenhang met de hoeveelheid persoonsgegevens en de verwerkingsdoelen zijn medebepalend voor de te nemen maatregelen
- de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de personen – feitelijk dient u een risico-inschatting te maken van uw verwerkingen en op basis hiervan uw maatregelen te treffen
- verwerkers – u kunt alleen een beroep doen op verwerkers die afdoende garanties met betrekking tot het toepassen van technische en organisatorische maatregelen bieden; deze maatregelen moeten worden opgenomen in een verwerkersovereenkomst; u bent bovendien gerechtigd te (laten) controleren bij uw verwerker(s) of de maatregelen adequaat zijn
- de uitvoeringskosten – de AVG biedt tevens ruimte om een kostenafweging te maken. Indien de risico’s beperkt zijn, wordt niet van u verwacht dat u grote investeringen doet om een hoog beschermingsniveau te bereiken.
- beleid – als u van mening bent dat u, gezien voorgaande zaken, hoge risico’s loopt bij de verwerking van persoonsgegevens, dan dient u een passend zogeheten gegevensbeschermingsbeleid uit te voeren. Dat houdt in dat u op basis van een risico-inschatting de beschermingsmaatregelen bepaalt. Voor de meeste mkb-ondernemingen zal een gegevensbeschermingsbeleid niet nodig zijn.

Maatregelen beveiligen
Vervolgens geeft de AVG enkele voorbeelden van mogelijke maatregelen, namelijk:

- pseudonimiseren en versleuteling van persoonsgegevens
- op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de systemen en diensten garanderen
- het tijdig herstellen van toegang en beschikbaarheid bij een incident, zoals een datalek
- een evaluatieprocedure om doeltreffendheid van de maatregelen te testen en beoordelen.

Pseudonimiseren van persoonsgegevens
Persoonsgegevens kunnen in het geval van pseudonimiseren niet meer aan een specifieke betrokkene worden gekoppeld zonder dat er aanvullende gegevens nodig zijn (een zogenaamde sleutel om informatie te decoderen). Omdat het via het gebruik van een sleutel nog steeds mogelijk is om de betreffende persoon (indirect) te identificeren, kwalificeren pseudoniemen nog steeds als persoonsgegevens. Dit in tegenstelling tot het anonimiseren van persoonsgegevens.

Andere maatregelen
Andere maatregelen die u sowieso moet treffen, zijn:

- wachtwoordbeleid en rechten- en autorisatiestructuur inrichten
- logging en controle (monitoring) van toegang tot de informatiesystemen
- implementatie van actuele beveiligingsupdates
- viruscontrole en firewall inregelen
- monitoring kwetsbaarheden op het interne en externe netwerk
- adequate fysieke beschermingsmaatregelen treffen

- procedures voor opslag, onderhoud en vernietiging van data opstellen
- procedures voor het behandelen van informatiebeveiligingsincidenten en datalekken opstellen
- back-upbeleid opzetten en uitvoeren adequate back-ups.

Gedragscode of certificering
Door als onderneming aan te sluiten bij een gedragscode voor de verwerking van persoonsgegevens (bijvoorbeeld binnen uw branche) of een specifieke certificering, kunt u aantonen dat u aan de vereisten voor technische en organisatorische maatregelen die de AVG stelt, voldoet. Een voorbeeld van een algemeen geaccepteerde standaard voor informatiebeveiliging is ISO27001.

Tip:
Indien u gebruik wilt maken van bepaalde certificeringen om wat betreft technische en organisatorische maatregelen te voldoen aan de verplichtingen uit de AVG, maak dan keuzes. Want het kan zijn dat uw onderneming niet alle onderdelen van die certificeringen nodig heeft!

2. Toch een datalek! Wat nu?

De AVG schrijft voor dat uw organisatie bepaalde inbreuken in verband met de verwerking van persoonsgegevens, zogenaamde datalekken, moet melden bij de Autoriteit Persoonsgegevens (AP). Wat betekent dit voor uw bedrijf? Waaraan moet u precies voldoen?

In sommige situaties dient u ook de betrokkene(n) bij het datalek te informeren. Deze verplichting is niet nieuw in de AVG en was ook al voorgeschreven in de Wet Bescherming Persoonsgegevens (WBP).

Wat is een datalek?
Een datalek wordt in de AVG (artikel 4) omschreven als ‘een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens’.

Er is alleen sprake van een datalek als zich een beveiligingsincident heeft voorgedaan én indien persoonsgegevens verloren zijn gegaan dan wel onrechtmatige verwerking van de persoonsgegevens redelijkerwijs niet uit te sluiten is.

Datalek snel melden
Indien een datalek heeft plaatsgevonden, meldt u deze zonder onredelijke vertraging, maar wel uiterlijk 72 uur nadat u er kennis van heeft genomen. Indien de melding aan de AP niet binnen 72 uur plaatsvindt, moet u motiveren waardoor de vertraging is opgetreden. Een (sub)verwerker, zoals een leverancier, moet u, omdat u verantwoordelijke bent, onverwijld te informeren zodra hij kennis heeft genomen van een datalek, zodat u nog de gelegenheid heeft tijdig de AP te informeren. Normaal gesproken maakt u hierover afspraken met uw verwerkers in een zogenaamde verwerkersovereenkomst. Het is dan ook raadzaam om met uw verwerker af te spreken dat deze uiterlijk binnen 24 uur aan u meldt, zodat u nog voldoende tijd heeft om te melden bij de AP.

Niet melden
Een datalek hoeft niet gemeld te worden als, zoals de AVG bepaalt, het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. In andere bewoordingen houdt dit in dat het datalek geen betrekking heeft op persoonsgegevens van gevoelige aard en/of het datalek niet leidt tot ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens of de kans hierop.

Persoonsgegevens van gevoelige aard en factoren met kans op ernstige nadelige gevolgen
Persoonsgegevens van gevoelige aard zijn:
- bijzondere persoonsgegevens zoals religieuze of levensbeschouwelijke overtuiging, ras, politieke opvattingen en gegevens over gezondheid
- BSN-nummer
- gegevens die kunnen leiden tot stigmatisering of uitsluiting
- gegevens die onderworpen zijn aan geheimhouding/beroepsgeheim

Factoren met (kans op) ernstige nadelige gevolgen:
- omvangrijke verwerkingen of een keten van gegevensverwerking
- ingrijpende beslissingen die worden genomen met de gegevens
- kwetsbare groepen zoals kinderen en gehandicapten

Hoe meld je een datalek?
Organisaties die een datalek moeten melden, doen dit bij de AP via het digitale meldingsformulier op de website van de AP. U kunt met dit formulier ook een voorlopige melding doen en deze later aanvullen of intrekken.

Welke informatie moet u verstrekken?
De volgende informatie moet u verstrekken:
- de aard van het datalek, waar mogelijk onder vermelding van de categorieën van betrokkenen en het aantal betrokkenen
- de naam van de persoon met wie contact kan worden opgenomen voor meer informatie
- de (waarschijnlijke) gevolgen van het datalek
- de maatregelen die u heeft voorgesteld en/of genomen om het datalek aan te pakken.

Documentatieplicht
Voor alle datalekken (ongeacht of u deze heeft gemeld) geldt dat u deze moet vastleggen in bijvoorbeeld een incidentenregister, waarbij u bovenstaande gegevens vastlegt. Daarbij is het raadzaam vast te leggen wat het meldingsnummer van het datalek is dan wel de reden waarom is besloten af te zien van melding.

Melding aan betrokkene
Wanneer een inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen (ofwel ongunstige gevolgen voor de persoonlijke levenssfeer van betrokkene), dient u de betrokkene(n) onverwijld te informeren. De mededeling aan de betrokkene bevat een toelichting – in duidelijke en eenvoudige taal – op wat er is gebeurd, op de acties en maatregelen die zijn ondernomen, wat het betekent voor de betrokkene en het advies dat u geeft over wat betrokkene het beste kan doen.

Let op!
In de volgende situaties dient altijd gemeld te worden aan betrokkene(n): het betreft lekken van persoonsgegevens van gevoelige aard, bijvoorbeeld BSN-nummers of financiële gegevens, de persoonsgegevens zijn blootgesteld aan vernietiging of aantasting of de versleuteling van de persoonsgegevens is niet adequaat of niet volledig.

Niet melden aan betrokkene
De mededeling aan de betrokkene(n) is niet vereist wanneer een van de volgende voorwaarden is vervuld:
- u heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling van gegevens
- u heeft achteraf maatregelen genomen om ervoor te zorgen dat het bedoelde hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen
- de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

3. Water of ijs op kosten van de zaak?

De mussen ‘vallen’ met deze hitte van het dak, maar als goed werkgever wilt u dat uw personeel zo weinig mogelijk last heeft van de hoge temperaturen. De airco staat natuurlijk aan, maar zijn er ook andere slimme tips of mogelijkheden binnen de werkkostenregeling?

Extra pauzes en tropenrooster
Een eenvoudige maatregel is het invoeren van extra pauzes. Of als het lukt met de werkzaamheden van uw organisatie: de introductie van een zogenaamd tropenrooster. Uiteraard doet u dit laatste in overleg met uw werknemers. Niet iedereen kan zijn werktijden immers zomaar aanpassen, bijvoorbeeld als je afhankelijk bent van het openbaar vervoer.

Voorkom uitdrogen
Een gevaar bij extreme warmte is de kans op uitdroging. Zorg voor voldoende water en/of deel frisdrank en thee uit. Op de werkplek kan dit onbelast. De 'werkplek' is iedere plek waar u als werkgever verantwoordelijk voor bent, dus bijvoorbeeld ook uw magazijn of vergaderruimte. U mag drankjes niet zomaar onbelast vergoeden, dus zorg dat u die zelf voor uw rekening neemt.

Werkkostenregeling
Is dit organisatorisch nogal lastig, dan kunt u drankjes ook vergoeden en de vergoeding onderbrengen in de werkkostenregeling. De vergoeding blijft dan voor de werknemer onbelast. Voor u als werkgever ook, mits u dit jaar aan vergoedingen en verstrekkingen niet meer uitgeeft dan 1,2% van de loonsom.

Let op!
Schiet u in de werkkostenregeling over de 1,2% van de loonsom, dan betaalt u als werkgever 80% eindheffing over het meerdere.

IJsje van de zaak
Ook een ijsje of andere koude versnapering zal zeker op prijs worden gesteld en komt de arbeidssfeer met deze warmte zeker ten goede. Ook dit blijft op de werkplek onbelast als uw bedrijf de rekening zelf betaalt. Een vergoeding is ook nu belast, dus liever niet.

4. Zo gaat de fiscus om met uw cryptovaluta

Sinds de spectaculaire waardestijging van de bitcoin, kunnen cryptovaluta rekenen op een toenemende belangstelling. Onlangs heeft ook de staatssecretaris van Financiën zich uitgelaten over de fiscale aspecten ervan.

Box 3
Duidelijk is in ieder geval dat het bezit van cryptovaluta moet worden opgegeven in box 3. De waarde op 1 januari van het betreffende jaar is beslissend. Cryptovaluta kunnen enorm fluctueren in waarde, wat betekent dat er enorme risico's aan verbonden zijn. Belastingplichtigen moeten er dan ook rekening mee houden dat een bezit aan cryptovaluta op 1 januari van een jaar 'zomaar' grotendeels verloren kan zijn op het moment dat er belasting over betaald moet worden.

Let op!
In voorkomende gevallen is het te overwegen alvast via een aanpassing van de voorlopige aanslag in te spelen op de waardestijging of -daling van de valuta.

'Minen' als inkomensbron?
Het verdienen van cryptovaluta via het zelf beschikbaar stellen van rekenkracht op een of meer computers, heet minen. Het is nog maar de vraag of minen door particulieren als inkomensbron moet worden aangemerkt en of het dus belast is. De staatssecretaris laat een duidelijk antwoord in het midden, maar geeft aan dat dit met name afhankelijk is van de vraag of voordeel redelijkerwijs te verwachten is. Gezien de onduidelijkheid rond de te verwachten voordelen, zal dit waarschijnlijk niet snel het geval zijn. Dit betekent echter ook dat verliezen niet aftrekbaar zijn.

Let op!
Voor bv's is minen een bedrijfsactiviteit en zijn de inkomsten dus altijd belast. Verliezen zijn dus ook aftrekbaar.

Ondernemers met cryptovaluta
Cryptovaluta worden nog slechts in uitzonderingsgevallen als betaalmiddel geaccepteerd. Cryptovaluta zijn voor ondernemers in het algemeen dan ook aan te merken als belegging. Verder zijn duurzaam overtollige liquide middelen voor ondernemers als privévermogen aan te merken. Dit betekent dat een speculatieverlies met cryptovaluta in de regel niet aftrekbaar is als verlies uit onderneming.

NIEUWSBERICHTEN

1. Te veel belasting over uw vermogen? Maak nu bezwaar!

Bent u het oneens met de berekening van de inkomstenbelasting over het rendement op vermogen (box 3-heffing) voor het belastingjaar 2017, dan moet u vanaf dit jaar altijd individueel en tijdig bezwaar maken tegen die aanslag. Tijdig wil zeggen binnen 6 weken na dagtekening aanslag. Voor aanslagen welke reeds opgelegd zijn voor eind mei, dagtekening brief inzake wijziging, geldt een verlenging termijn zodat het bezwaar vóór 15 juli binnen moet zijn. Dit heeft de Rijksoverheid laten weten. De heffing over ons vermogen in box 3 wordt gebaseerd op een forfaitair rendement. Of u dat rendement in werkelijkheid ook behaalt, is niet van belang.

Eerder is beslist dat bezwaren tegen de heffing op spaarsaldi in box 3 worden aangemerkt als 'massaal bezwaar' voor de periode 2013 tot en met 2016. Dit betekent dat bezwaren tegen de heffing in box 3 over deze jaren niet nodig zijn, voor zover het de heffing op spaarsaldi betreft. Worden belastingplichtigen in deze zaken in het gelijk gesteld, dan geldt de uitspraak dus voor iedereen in soortgelijke omstandigheden.

2. Publicatieplicht jaarcijfers anbi vóór 1 juli

Een anbi is een Algemeen Nut Beogende Instelling die een aantal fiscale voordelen geniet. Daar zitten wel voorwaarden aan vast. Een anbi is verplicht de balans en de staat van baten en lasten van een jaar binnen zes maanden te publiceren. Voor 2017 betekent dit dat de cijfers vóór 1 juli 2018 gepubliceerd moeten zijn. Ook moet een toelichting hierop worden gepubliceerd. Let op: de gegevens moeten gepubliceerd worden op een internetsite.

Naast de jaarlijkse cijfers moeten ook de volgende gegevens standaard op de site vermeld worden: naam en contactgegevens van de anbi, RSIN/fiscaal nummer, omschrijving doelstellingen, een beleidsplan, bestuurders plus hun functie, beloningsbeleid bestuur, directie en personeel en een verslag van de uitgeoefende activiteiten.

3. AVG-regels als uw werknemer vertrekt

Uw werknemer die beschikt over belangrijke persoons- en privacygevoelige gegevens, gaat het bedrijf verlaten. U wilt niet dat uw bedrijfsgegevens op straat komen te liggen. Neem daarom maatregelen en maak goede afspraken met uw (ex-)werknemer.

Hoe vaak gebeurt het niet dat als een werknemer uit dienst is, hij nog kan inloggen op het ICT-systeem van een bedrijf? Heeft u de login van de bedrijfspagina voor deze werknemer op social media geblokkeerd? Heeft u ook gedacht aan de login van ICT-netwerken van bedrijven waarmee u samenwerkt? Maak daarom afspraken en tref de benodigde maatregelen als uw werknemer uit dienst gaat.

Waaraan moet u denken? Zorg ervoor dat uw (ex-)werknemer op de datum dat hij uit dienst gaat, bedrijfseigendommen, zoals usb-sticks, een laptop, mobiele telefoon en desktop, inlevert. Daarnaast dient u ervoor te zorgen dat de ex-werknemer niet meer kan inloggen op het netwerk van uw bedrijf, niet meer kan inloggen op de sociale media van uw bedrijf of andere ICT-netwerken van bedrijven waarmee u samenwerkt. Vraagt u zich ook af of de (ex-)werknemer elders, bijvoorbeeld thuis, beschikt over privacy- en persoonsgevoelige informatie.

Neem in de beëindigingsovereenkomst op dat als de ex-medewerker alsnog bij privacy- en persoonsgevoelige informatie kan, de ex-medewerker uw bedrijf hiervan onmiddellijk op de hoogte brengt.

4. Ontslag op staande voet: toch transitievergoeding?

Als u als werkgever de arbeidsovereenkomst met een werknemer, die ten minste twee jaar in dienst is, opzegt, bent u een transitievergoeding verschuldigd. Daarop is een uitzondering, namelijk in het geval dat het ontslag het gevolg is van ernstig verwijtbaar handelen of nalaten van uw werknemer. Bij een ontslag op staande voet is daarvan vaak sprake, maar let op: niet in alle gevallen! Een dringende reden die een ontslag op staande voet rechtvaardigt, hoeft niet automatisch te betekenen dat de werknemer ook ernstig verwijtbaar heeft gehandeld. De Hoge Raad heeft in een recente zaak geoordeeld dat het niet zo is dat er nooit een transitievergoeding verschuldigd is bij een ontslag op staande voet. Of u een transitievergoeding moet betalen, hangt dan namelijk af van het feit of de werknemer ernstig verwijtbaar heeft gehandeld. Als dit niet het geval is, bent u toch transitievergoeding verschuldigd.

In de recente rechtszaak ging het om een werknemer die meerdere keren, ondanks officiële waarschuwingen en alcoholprotocollen, onder invloed van alcohol op het werk was verschenen en daardoor op staande voet werd ontslagen. Volgens de Hoge Raad is door de kantonrechter en het gerechtshof niet afzonderlijk beoordeeld of hier wel sprake was van ernstig verwijtbaar handelen van de werknemer. De werknemer stelde zich namelijk op het standpunt dat hem vanwege zijn alcoholverslaving geen verwijt, of in zeer geringe mate een verwijt, kon worden gemaakt.

5. Zonnepanelen verhogen WOZ-waarde

Als u zonnepanelen op uw pand plaatst, verhoogt dit de WOZ-waarde. Dit blijkt uit een recente uitspraak van het gerechtshof. Van belang was dat ze 'duurzaam', dus voor onbepaalde tijd, geïnstalleerd waren. De zonnepanelen werden als onroerend aangemerkt. In deze zaak betrof het niet-geïntegreerde zonnepanelen, ze lagen los op het dak. Ook voor wel geïntegreerde zonnepanelen mag daarom worden aangenomen dat deze als onroerend worden aangemerkt. Dat de technische mogelijkheid bestond dat de zonnepanelen bij verhuizing mogelijk zouden worden meegenomen, achtte het Hof niet van belang.

In de betreffende zaak was de conclusie dat de WOZ-waarde niet te hoog was vastgesteld. De gevolgen strekken echter verder dan alleen de WOZ en OZB. De WOZ-waarde is namelijk ook bepalend voor de hoogte van het eigenwoningforfait (EWF), dat voor de meeste woningen in 2018 0,7% van de WOZ-waarde bedraagt.

6. Hypotheek in 40 jaar aflossen?

De meeste mensen lossen hun hypotheek in 30 jaar af. Maar er zijn nieuwe producten op de markt, waarbij deze termijn verlengd is naar 40 jaar. Wat zijn daarvan de voor- en nadelen?

Het voordeel van een langere looptijd is dat de maandlasten lager zijn, omdat de aflossing over een grotere periode kan worden gespreid. Dit is vooral voor starters op de woningmarkt van belang, zeker nu koopwoningen fors in prijs stijgen. Wel betaal je over een langere periode rente, en dus in totaal meer rente. Een langere aflossingstermijn is ook verdedigbaar met het oog op de latere AOW- en pensioendatum die tegenwoordig geldt. Wie later met pensioen gaat, kan ook langer doen over het aflossen van zijn hypotheek.

Let op: sinds 2013 geldt voor nieuwe hypotheken een verplichte aflossing van de verstrekte som in maximaal 30 jaar. Als u een lineaire of annuïteitenhypotheek afsluit, wordt aan deze voorwaarde voldaan. Een hypotheek met langere looptijd dan 30 jaar is hiermee in strijd. Dit zou betekenen dat de hypotheekrente dan niet aftrekbaar is. Om dit probleem te omzeilen, wordt bij deze hypotheek de hoofdsom in twee delen gesplitst: een aftrekbaar deel dat in 30 jaar helemaal wordt afgelost, en een niet-aftrekbaar deel dat 40 jaar loopt. De bruto maandlasten van het totaal blijven 40 jaar gelijk.