IT solutions in green

TIPS

TSD levert totaaloplossingen voor ICT in de groene sector. Daarbij volgen wij continu marktontwikkelingen, evenals andere actualiteiten die daarmee sterk in verband staan. De GDPR (General Data Protection Regulation) ofwel de Nederlandse AVG (Algemene Verordening Gegevensbescherming) is erg actueel. Verplichte wetgeving waar alle organisaties en bedrijven aan moeten voldoen en raakvlakken met ICT heeft. Maar de ICT, ofwel de techniek, is niet het enige.

Voldoen aan de AVG betekent iets voor mens, proces en techniek. Hierdoor kan de nieuwe wet- en regelgeving als complex worden ervaren. Ook al hebben wij “AVG-ondersteuning” niet aan de dienstverlening van TSD toegevoegd, daar zijn andere specialisten voor; wij helpen onze relaties wel graag een beetje op weg.

Vragen als…

- Wat betekent het voor mij?
- Wat moet ik nu exact doen?
- Waar moet ik beginnen?

… worden namelijk wel aan ons gesteld door relaties.

Wij hebben voor onze relaties daarom eerder presentaties laten verzorgen door Sebyde over dit onderwerp. Sebyde heeft zich wel gespecialiseerd in ondersteuning op het gebied van de AVG. Welke specialist je ook inschakelt of wanneer je volledig zelfstandig de AVG binnen jouw organisatie oppakt; er is voorbereiding nodig. De eerste stap is een risico-inventarisatie en daarvoor is veel informatie nodig. Om te komen tot de verzameling gegevens voor de risico-inventarisatie hebben we een aantal tips samengesteld. De vraag “waar moet ik beginnen” kun je daarmee beantwoorden. Met de uitkomst hiervan is een basis gelegd voor het vervolg. Op welke manier je dat ook wilt doen.

“Waar moet ik beginnen”, begint met deze voorbereiding nadat je de toelichting “de AVG; wat betekent dat voor u…”, die je hierbij als bijlage hebt gekregen, hebt gelezen. Voor meer informatie raden we je ook de website van de Autoriteit Persoonsgegevens aan.

TSD IT bv
Schrevenweg 4
8024 HA Zwolle
The Netherlands
Postbus 30101
8003 CC Zwolle
The Netherlands
Tel +31 38 850 50 50
Fax +31 38 850 50 55
E-mail info@tsd.nl
Web www.tsd.nl
Support
Fax +31 38 454 24 12
E-mail support@tsd.nl
VAT NL8000.19.891.B01
Bank 67.38.21.781
Swift INGBNL2A
Iban NL48 INGB 0673 8217 81

IT solutions in green

Tip 1: “in beeld brengen”

Inleiding bij Tip 1:

Wat zijn persoonsgegevens binnen de AVG?

De AVG (GDPR) heeft betrekking op persoonsgegevens. Persoonsgegevens zijn gegevens die direct of indirect herleidbaar zijn naar een natuurlijk persoon. Een bedrijfsnaam “Boomkwekerij B.V.” is geen persoonsgegeven, de heer K. Lant of mevrouw B. Oom is dat wel. Persoonsgegevens kunnen ook bijzonder gevoelig zijn. Onder die criteria vallen gegevens die, bij het lekken daarvan, inbreuk kunnen maken op de privacy van mensen en veel negatieve invloed zou kunnen hebben. Zoals bijvoorbeeld; gegevens over ziekteverzuim of een burgerservicenummer (BSN: let op: het BTW-nummer van een ZZP-er is gemakkelijk te herleiden naar het BSN). Gegevens dus die de meeste bedrijven van hun medewerkers, maar ook eventuele inhuurkrachten, in bezit hebben. Persoonsgegevens in de categorie “bijzonder” mag je niet verwerken tenzij daar een specifieke gerechtvaardigde grondslag voor is (zoals bijvoorbeeld een arbeidscontract met een medewerker).

Maar een persoonsgegeven is bijvoorbeeld ook het zakelijk e-mailadres van iemand dat persoonsgebonden is, k.lant@boomkwekerij.nl. Zo’n e-mailadres valt niet onder de categorie “bijzonder”, maar is wel een persoonsgegeven en valt onder de reikwijdte van de AVG. Persoonsgegevens die niet in de categorie “bijzonder” vallen, mogen wel verwerkt worden en daarvoor moet ook een gerechtvaardigde grondslag zijn. Voor alle type persoonsgegevens geldt dat de organisatie die deze in bezit heeft verantwoordelijk is voor de verwerking van die gegevens. Binnen de AVG wordt dat “verwerkingsverantwoordelijke” genoemd.

Wat is verwerken volgens de AVG?

In de AVG wordt gesproken over “verwerken”. Dit is feitelijk alles dat je met een gegeven kan doen. Denk daarbij aan: bewaren, bewerken, kopiëren, vernietigen, bericht sturen etc. Om binnen de AVG persoonsgegevens te mogen “verwerken” moet er dus een gerechtvaardigde grondslag zijn. Een arbeidsovereenkomst met een medewerker is dus bijvoorbeeld een gerechtvaardigde grondslag om persoonsgegevens van een medewerker te mogen verwerken. Een zakelijke relatie, zakelijke overeenkomst, vormt de grondslag voor het verwerken van (persoons)gegevens maar de gegevens mogen niet buiten de relevantie vallen.

Een voorbeeld: een gepersonaliseerd e-mail adres (zoals k.lant@boomkwekerij.nl) heeft die relevantie als het gaat om een klant die bomen bij je koopt, maar het bewaren van informatie over het lidmaatschap van een vakbond (voor zover je dat al weet) van die specifieke persoon niet.

Daarnaast kan expliciete toestemming de gerechtvaardigde grondslag zijn om geïnteresseerden (leads/prospects) regelmatig een nieuwsbrief te sturen.
Dan is er (nog) geen zakelijke overeenkomst, er wordt nog geen zaken gedaan, maar iemand heeft bijvoorbeeld op een contactformulier van jouw website aangegeven een nieuwsbrief van jouw bedrijf per e-mail te willen ontvangen. Toestemming is dan de gerechtvaardigde grondslag om gegevens te mogen verwerken (opt-in wordt dit genoemd).

IT solutions in green

Waarvoor mogen persoonsgegevens worden gebruikt?

De gegevens mogen alleen gebruikt worden voor het doel waarvoor ze zijn toevertrouwd. Stel dat iemand expliciet heeft aangegeven graag informatie te willen ontvangen over het aanbod van planten en bomen dan mag iemand niet zomaar worden aangeschreven voor iets dat daar niets mee te maken heeft. Dat geldt niet alleen voor iemand die zich als “geïnteresseerde” heeft gemeld, maar ook voor bestaande relaties, klanten waarmee je al zaken doet. Als er een zakelijke overeenkomst (gerechtvaardigde grondslag) is voor het leveren van groen mag niet zomaar iemands persoonsgegeven worden gebruikt om te benaderen voor bijvoorbeeld een lidmaatschap voor een leuk tijdschrift. Om maar iets te noemen.

Kortom, de wijze waarop de persoonsgegevens gebruik worden moeten in relatie staan met de gerechtvaardigde grondslag. Het kan dus zijn dat er een zakelijke relatie is met iemand voor alleen de aankoop van planten of bomen en dat die klant heeft aangegeven open te staan voor het aanbod van andere diensten/producten van jouw bedrijf. Dan is er naast de zakelijke verbinding/overeenkomst (het kopen van groen) ook toestemming (het versturen van marketingberichten). Bij het benaderen van personen namens een bedrijf, ter attentie van iemand persoonlijk dus, geldt deze specifieke toestemming. Het gaat hier immers om persoonsgegevens die gebruikt worden om iemand te benaderen.

Nog wat meer over de gerechtvaardigde grondslag in geval van een ander soort verwerking van persoonsgegevens. Bijvoorbeeld de verwerking van personeelsgegevens. Die worden gebruikt voor onder andere het kunnen betalen van het salaris, het kunnen begeleiden van ziekteverzuim, informatie over het functioneren of mutaties binnen pensioenen etc. Hiervoor is de arbeidsovereenkomst een gerechtvaardigde grondslag. Persoonsgegevens in het algemeen mogen niet zomaar gedeeld worden met anderen (externe bedrijven). Dat mag wel indien daarvoor een grondslag, is zoals bijvoorbeeld het uitbesteden van werkzaamheden die namens/in opdracht van jou worden uitgevoerd.

Bijvoorbeeld; het overdragen van een personeelsbestand aan een adviseur die medewerkers gaat benaderen voor een aanbieding die niets met de arbeidsovereenkomst te maken heeft, is dus niet in lijn met de AVG. Een arbo-arts die een medewerker benadert in het kader van ziekteverzuim en re-integratie is wel toegestaan. Sterker nog, de werkgever heeft een verplichting tot begeleiding ter vermindering van ziekteverzuim en ter bevordering van re-integratie en mag hiervoor een externe specialist betrekken. Het delen van persoonsgegevens is dus toegestaan indien er sprake is van het “uitbesteden” van een taak die past bij de grondslag en namens/in opdracht van jou gebeurt. Met zo’n partij moeten wel hele specifieke afspraken worden gemaakt en vastgelegd. Dat onderwerp komt in de volgende “tip” aan de orde.

Hoe zit het met het bewaren van persoonsgegevens?

Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk, verplicht of gewenst is. Dit betekent dat wanneer zo’n geïnteresseerde aangeeft niet meer in het “mailingbestand” opgenomen te willen zijn, deze gegevens op diens verzoek verwijderd moeten worden. Het recht op het laten verwijderen van persoonsgegevens geldt in alle gevallen. Zo’n verzoek moet ook binnen 4 weken geregeld worden.

Behalve wanneer er een wettelijke plicht is om gegevens toch te bewaren. Het bewaren van die gegevens heeft dan een andere (verplichte) grondslag. Denk hierbij bijvoorbeeld aan een ex-medewerker die terstond na uit dienst treden verzoekt om het verwijderen van diens gegevens. Wettelijke bepalingen geven aan dat personeelsgegevens een bepaalde periode bewaard moeten blijven. Zo'n verzoek van verwijdering kan dan niet gehonoreerd worden. Uiteraard blijven de criteria van relevantie en vertrouwelijkheid onherroepelijk van kracht.

Samenvattend:

Persoonsgegevens mogen alleen verwerkt worden als er een gerechtvaardigde grondslag voor is. De persoonsgegevens die je bewaart, moeten relevant zijn voor het doel van de verwerking en mogen alleen verwerkt worden voor dát doel. Deze gegevens mogen niet langer bewaard worden dan noodzakelijk, verplicht of gewenst is. Een verzoek tot verwijdering van gegevens moet worden uitgevoerd, tenzij er een andere verplichting is om de gegevens te (moeten) bewaren. Persoonsgegevens mogen alleen worden gedeeld met andere bedrijven (externen) als daarvoor een gerechtvaardigde grondslag is, zoals het uitbesteden van een taak, waarbij de verwerkingsverantwoordelijke verantwoordelijk blijft voor het borgen van de veiligheid van de persoonsgegevens.

Tip 1: Breng in kaart:

- Welke persoonsgegevens heb ik?
- Hoe lang bewaar ik die persoonsgegevens?
- Hoe kom ik aan die persoonsgegevens?
- Waar gebruik ik die persoonsgegevens voor?
- Gebruik ik de persoonsgegevens volgens de gerechtvaardigde grondslag die ik heb?

IT solutions in green

Tip 2:

Vertrouwelijk omgaan met gegevens:

Met alle persoonsgegevens moet vertrouwelijk worden omgegaan. Dit betekent dat het nooit zomaar aan een andere (derde) partij mag worden gegeven (tenzij daar een gerechtvaardigde grondslag voor is, zoals uitbesteding van een taak). Een goede autorisatie binnen de systemen (techniek) in de eigen organisatie is om te beginnen heel belangrijk. Een autorisatie die past bij de functie van mensen. Menselijk handelen, en vaak ook nog onbedoeld, kan leiden tot datalekken (het lekken van gegevens). Een autorisatie die niet aansluit op de functie en daarmee kennis en kunde kan dan een groot risico zijn. Een goede autorisatie binnen het bedrijf helpt om te voorkomen dat gegevens (onbedoeld) in verkeerde handen vallen of dat je niet weet waar deze terecht kunnen komen.

Maar ook externen (partijen waar je taken aan uitbesteed) zijn daarbij relevant. Als gebruik wordt gemaakt van andere bedrijven die toegang hebben tot persoonsgegevens is het belangrijk om er (zo) zeker (mogelijk) van te zijn dat deze partij de gegevens net zo zorgvuldig behandelt (verwerkt) als je dat binnen jouw eigen organisatie wilt. En belangrijker: persoonsgegevens waar jij verantwoordelijk voor bent. Want ook al besteed je werkzaamheden uit; jij blijft verantwoordelijk voor de persoonsgegevens die jou zijn toevertrouwd. Sterker nog, binnen de AVG is het verplicht om met externe partijen een verwerkersovereenkomst te regelen waarin die “zorgvuldigheid” concreet wordt afgesproken. Externe partijen (bedrijven) die voor een uitvoerende dienst ingehuurd worden, worden in de AVG “verwerkers” genoemd.

Voorbeeld 1: Laten we eens kijken naar gegevens van medewerkers en/of inhuurkrachten. Dat zijn dus vaak “bijzondere” gegevens; BSN, banknummer, geboortedatum, verzuiminformatie, salarisgegevens, informatie over het functioneren etc. Veel bedrijven laten hun salarisadministratie uitvoeren door een administratie/accountantskantoor. Deze heeft dan de beschikking over bijzondere persoonsgegevens van jouw medewerkers waar jij verantwoordelijk voor bent. Met zo’n partij moet er daarom een overeenkomst zijn waarin afspraken worden gemaakt over de veiligheid van die persoonsgegevens. Denk in deze richting ook aan een arbodienst of een adviseur die de pensioenen regelt. Maar er zijn mogelijk meer partijen. Wanneer je dergelijke gegevens digitaal binnen jouw netwerk bewaart, kunnen andere partijen die daartoe toegang (kunnen) hebben deze ook inzien. Zoals bijvoorbeeld een systeembeheerder. Ongeacht of deze partij deze gegevens inhoudelijk zal bekijken, heeft die partij wel de mogelijkheid. Een dergelijke partij zal daarom ook de uiterste zorgvuldigheid met jouw bedrijf overeen moeten komen. Kortom, bedenk wie toegang zou kunnen hebben tot die gegevens.

Voorbeeld 2: Stel dat je op jouw netwerk een bestand bijhoudt van geïnteresseerden, leads of prospects (hoe je ze ook noemt). Iedere maand stuur je deze geïnteresseerden een op naam gepersonaliseerde nieuwsbrief (waarvoor ze toestemming hebben gegeven) naar hun gepersonaliseerde e-mailadres. Om dat op een handige en mooie manier te doen, maak je gebruik van een marketing-e-mailfunctie. Een voorbeeld daarvan is “mailchimp”. Persoonsgegevens, ook al zijn ze waarschijnlijk niet bijzonder gevoelig, worden dan gekoppeld aan die (online)functie (Mailchimp). Wanneer je gaat inventariseren wie bij dit soort gegevens kan, moet dan ook aan een

partij als (voorbeeld) "mailchimp" worden gedacht. Maar evengoed de beheerder van de netwerk-ICT-omgeving, zoals in het vorige voorbeeld aan de orde kwam.

De digitale, online, door internet gefaciliteerde wereld of locatieonafhankelijk werken, hoe je het maar wil noemen, is een groot risico als het gaat om de mogelijkheid dat data (dus ook persoonsgegevens) in verkeerde handen komt. De bedrijven waar geen internet aanwezig is, zijn waarschijnlijk op één hand te tellen (als ze er al zijn). Internet is een risico, dat weten we allemaal. Of je nu "in de cloud" werkt, een fysiek eigen serverpark of (verschillende stand alone) PC's hebt. Of je veel beheer zelf "in huis" doet, een systeembeheerder voor de hardware en infrastructuur hebt of een softwareleverancier die je helpt bij het gebruik van jouw administratiesysteem; bij het werken met een dienstverlener zal je zeker moeten weten dat deze partij zorgvuldig omgaat met jouw persoonsgegevens en zorgt voor een optimale beveiliging op het niveau dat past binnen hetgeen jij van die partij afneemt. Wanneer een softwareleverancier bijvoorbeeld verbinding maakt om in jouw bedrijfsadministratie mee te kijken bij een vraagstuk in de software, moet je geregeld hebben dat deze dat met optimale veiligheid doet. Als je een clouddienst afneemt, zal je er op moeten kunnen vertrouwen dat deze partij de best haalbare voorzieningen in stand houdt om de veiligheid van jouw data te borgen. En wanneer je de personeelsgegevens aanreikt aan een arbodienst moet jij ervan overtuigd zijn dat deze partij dat doet op de meest veilige manier die haalbaar is. Met dit soort partijen regel je daarom de verwerkersovereenkomst; daarin maak je afspraken over hoe die partijen omgaan met de persoonsgegevens waarvoor jij verantwoordelijk bent. Dat is niet alleen verstandig om te doen; het is binnen de AVG ook verplicht.

Samenvattend:

De "eigenaar" van de gegevens is en blijft de verwerkingsverantwoordelijke. Deze kan taken uitbesteden aan externe bedrijven. Deze taken worden dan door die externe, binnen de AVG "verwerker" genoemd, uitgevoerd in opdracht van verwerkingsverantwoordelijke. Als met een verwerker wordt gewerkt, moet er een verwerkersovereenkomst gerealiseerd zijn tussen partijen.

Tip 2 is om in kaart te brengen:

- Wie binnen (intern) de organisatie bij welke gegevens kan en of dat klopt met de functie/taak die beoefend wordt (autorisatie).
- Wie buiten de organisatie bij de persoonsgegevens kan en of er met die partij een verwerkersovereenkomst geregeld zou moeten worden.
  (Denk bijvoorbeeld aan: systeembeheerder, softwareleverancier, arbodienst, salarisadministratiekantoor, pensioenadviseur etc).
- Denk er ook over na of jouw onderneming als "verwerker" zou kunnen worden aangemerkt (heb jij toegang tot persoonsgegevens van andere bedrijven?)

IT solutions in green

Tip 3:

Hoe zit het met de digitale veiligheid?

Eenmaal wetende welke persoonsgegevens we hebben, wat we ermee doen en wie daar allemaal bij kunnen, is het goed om te inventariseren welke maatregelen je zelf hebt getroffen op technisch niveau. Dit is geen statisch gebeuren. Periodiek zal gevolgd moeten worden of de maatregelen nog voldoen. Hierbij kun je denken aan het treffen van maatregelen zoals adequate viruspreventie, het actueel houden van de digitale voorzieningen (update/patches in software) en de back-up voorzieningen.

Daarnaast is het essentieel om ervoor te zorgen dat de data (in het kader van de AVG gaat het dus om persoonsgegevens, maar uiteindelijk betreft het alle essentiële bedrijfsgegevens als het gaat om bedrijfsbelangen) beschikbaar blijft.

Hoe gaan de mensen in de organisatie er mee om?

Naast het regelen van autorisaties binnen functies in de onderneming, afspraken met andere bedrijven die de persoonsgegevens kunnen benaderen en hoe goed de techniek is ingericht, speelt natuurlijk ook hoe jij en jouw medewerkers er zelf mee omgaan een grote rol. Als een medewerker een mobiele telefoon heeft met toegang tot het bedrijfsnetwerk dan is er sprake van een datalek als zo'n apparaat gestolen wordt. Een dief kan dan immers toegang hebben tot de bedrijfsgegevens en mogelijk ook persoonsgegevens. Maar ook hard copy's. Een print van het personeelsbestand met vertrouwelijke gegevens in zijn geheel bij het oud papier is een vorm van het lekken van persoonsgegevens. Een datalek. Een gestolen laptop, USB-stick etc. Dit is vooral het organisatorische deel; hoe gaat iedereen ermee om? Bewustwording is daarbij erg belangrijk. Dat iedereen weet welke risico's er zijn in de dag van vandaag en daarop let. Elkaar oplettend houden: bewust maken en blijven.

Het is vooral logisch nadenken over: waar het mis kan gaan, elkaar bewustmaken (kennis delen) en welke afspraken je met elkaar maakt (en vastlegt) over hoe je ermee omgaat. Belangrijk is ook dat ("een ongeluk zit immers in een klein hoekje") je met elkaar afspraken maakt over wat te doen wanneer (je het vermoeden hebt dat) het is misgegaan. Tot wie je je dan moet wenden binnen het bedrijf: die weet hoe er dan gehandeld moet worden. Dat het geen "taboe" is maar dat je "dat ongelukje" gewoon deelt. Het kan echt namelijk iedereen overkomen!
Medewerkers in het bedrijf zijn toegewijd en betrouwbaar; daar gaat iedere ondernemer vanuit en zo moet het ook; anders kun je immers niet samenwerken. Toch kan het belangrijk zijn om dat nog even aan het papier toe te vertrouwen. Het kan raadzaam zijn om medewerkers (vaste en al dan niet tijdelijke of inhuur/uitzendmedewerkers) een geheimhoudingsverklaring te laten ondertekenen. In ieder geval de mensen in jouw bedrijf die toegang hebben tot persoonsgegevens. Niet alleen om de afspraken onderling vast te leggen, maar ook om aan te tonen dat je als bedrijf de uiterste zorgvuldigheid in acht neemt. Dat is wat de AVG (aantoonbaar) verlangt van ons allen.

IT solutions in green

Tip 3 is het in kaart brengen van:

- Wat er aan voorzieningen is getroffen in het “digitale park”?
- Welke risico’s schat je zelf in “als het misgaat”?
- Welke voorzieningen daarvoor getroffen zijn?
- Wie erop past dat de voorzieningen zoals die gewenst zijn ook in stand blijven. “Wie klaart deze klus en/of stuurt dat aan als je dat hebt uitbesteed?”
- Hoe veilig gaan wij er zelf mee om?
  Een tip om daarmee te beginnen is om tijdens bijvoorbeeld een koffiemoment met medewerkers/teams enige discussiepunten te bespreken. Eén persoon uit de groep maakt een verslagje van deze “sessie” en dat bewaar je bij verzamelde informatie.
- Benoem ook een persoon (en een back-up persoon; iedereen is immers wel eens op vakantie…) om een eventuele “probleemsituatie” te begeleiden.

TSD IT bv
Schrevenweg 4
8024 HA Zwolle
The Netherlands
Postbus 30101
8003 CC Zwolle
The Netherlands
Tel +31 38 850 50 50
Fax +31 38 850 50 55
E-mail info@tsd.nl
Web www.tsd.nl
Support
Fax +31 38 454 24 12
E-mail support@tsd.nl
VAT NL8000.19.891.B01
Bank 67.38.21.781
Swift INGBNL2A
Iban NL48 INGB 0673 8217 81

IT solutions in green

Tip 4:

Welke informatie moet gegeven worden over persoonsgegevens?

Nu in beeld is gebracht welke persoonsgegevens er zijn, wie daarbij kunnen, hoe daarmee wordt omgegaan, hoe de inrichting is, hoe medewerkers zich gedragen, is het ook van belang om dat kenbaar te maken. Transparantie dus. Een privacyverklaring moet beschikbaar zijn op de website. In deze verklaring staat waarvoor persoonsgegevens worden gebruikt, hoe eventuele cookies worden ingezet, of er sprake is van het volgen van internet gedrag etc.

Hoe zit het met de rechten van betrokkenen?

De rechten van betrokkenen (mensen van wie de persoonsgegevens zijn) zijn in de AVG strak weergegeven. Zo heeft iemand het recht op inzage. Iemand kan vragen om inzicht in welke persoonsgegevens er van hem of haar binnen jouw administratie worden bewaard. Iemand kan verzoeken om correctie van die gegevens, maar ook om deze te verwijderen. Een verzoek is dan feitelijk een opdracht. Hieraan moet gehoor worden gegeven binnen 4 weken. Het is daarom goed dat binnen jouw bedrijf bekend is dat dergelijke verzoeken kunnen komen en hoe daarmee moet worden omgegaan. Belangrijk is ook om te weten dat als er een verzoek tot verwijdering komt; dit voor alle samenwerkende partijen geldt. Stel dat iemand die als “geïnteresseerde” in jouw bestand is opgenomen voor marketingactiviteiten verzoekt om verwijdering van gegevens dan moet dat verzoek ook worden gehonoreerd door een samenwerkende partij. Dat zou bijvoorbeeld een marketingbedrijf kunnen zijn die je gebruikt om de maandelijkse nieuwsbrief te verzorgen. Als jij, als “verwerkingsverantwoordelijke”, een dergelijk verzoek moet uitvoeren; dan moet je ervoor zorgen dat ook de “verwerkers” waar jij gebruik van maakt dat verzoek uitvoeren.

Hoe te werken met opt-in en opt-out?

Het aan- of afmelden voor marketing moet dus mogelijk zijn. Dit is al in Tip 1 aan bod gekomen. Marketingberichten mogen alleen verstuurd worden naar personen die daar toestemming voor hebben gegeven (opt-in) en ieder persoon moet de mogelijkheid hebben om het ook weer te stoppen (opt-out). Het moet aantoonbaar zijn dat er een gerechtvaardigde grondslag is als iemand wordt benaderd met marketinguitingen (toestemming). Belangrijk dus om in de administratie te registreren óf er een opt-in is, waarvoor en per wanneer en eventueel een opt-out.

Tip 4 zijn de volgende acties:

- Kijk eens of jouw privacyverklaring actueel is (maak een exemplaar als deze er nog niet is of zet de actie op de “to-do-list” als je hiervoor expertise van anderen wilt inschakelen).
- Zorg ervoor dat deze op jouw website(s) beschikbaar is en zorg ervoor dat medewerkers ook op de gepresenteerde manier handelen.
- Is iedereen binnen de organisatie ervan op de hoogte dat er rechten als inzage, correctie en verwijdering zijn (kennis delen)?
- Is er een werkproces dat regelt dat aan die inzage, correctie en verwijdering adequaat gehoor kan worden gegeven?
- Bieden wij de gelegenheid tot opt-in en opt-out op een eenvoudige en duidelijke wijze?

TSD IT bv
Schrevenweg 4
8024 HA Zwolle
The Netherlands
Postbus 30101
8003 CC Zwolle
The Netherlands
Tel +31 38 850 50 50
Fax +31 38 850 50 55
E-mail info@tsd.nl
Web www.tsd.nl
Support
Fax +31 38 454 24 12
E-mail support@tsd.nl
VAT NL8000.19.891.B01
Bank 67.38.21.781
Swift INGBNL2A
Iban NL48 INGB 0673 8217 81

- Is de opt-in en opt-out goed in onze administratie verwerkt (inrichting van de techniek en het werkproces)?

IT solutions in green

Tip 5:

Het is misgegaan: er is (vermoeden van een) een datalek. Wat nu?

Wat is een datalek? Iets om mee te beginnen. Een datalek in de zin van de AVG is het lekken van persoonsgegevens ten gevolge van een beveiligingsincident. Dit beveiligingsincident kan technische of organisatorische oorzaken hebben, maar ook ontstaan door menselijk handelen. Nogal breed dus. In het kader van de AVG moet dan beoordeeld worden:

a. Is er sprake van een beveiligingslek?
b. Is er sprake van het (mogelijk) lekken van persoonsgegevens?

Als de antwoorden daarop "ja" luiden, dan moet gehandeld worden volgens de Meldplicht Datalekken.

En hoe borg je dat in jouw organisatie?

1. Zorg ervoor dat mensen in de organisatie weten wat een datalek is.
2. Zorg ervoor dat er één of meerdere (al dan niet als back-up) personen zijn die weten hoe te handelen volgens de regelgeving én vooral dat alle mensen binnen de organisatie weten tot wie ze zich direct na ontdekken moeten wenden.
3. Zorg ervoor dat, indien je die expertise zelf niet in jouw bedrijf hebt, er een partij is tot wie je je kunt wenden voor advies. Acteer direct!

Afhankelijk van het type datalek zal immers de vervolgactie bepaald moeten worden. Is er sprake van ransomware dan zijn de handelingen waarschijnlijk anders dan wanneer iemand een USB-stick is verloren. Een FG (functionaris gegevensbescherming) zal weten welke acties moeten worden ondernomen en op welk moment. Maar niet iedere organisatie heeft een FG en het is voor veel MKB-bedrijven ook niet verplicht. Op de website van de Autoriteit Persoonsgegevens is te lezen voor welke organisaties het verplicht is. Een interne FG of niet: het niet voldoen aan de Meldplicht kan grote consequenties hebben. Het is daarom wel belangrijk om een "stakeholder" intern in de organisatie te hebben die weet wat te doen en wanneer. Die "stakeholder" kan de begeleider zijn en iemand (bijvoorbeeld een externe adviseur) inschakelen als dat nodig is.

Tip 5 is daarom:

- Om te beoordelen wie het interne aanspreekpunt zal zijn in het geval van Datalekken.
- Om te beoordelen of het nodig is om een externe partij "paraat" te hebben in zo'n geval.
- Om te bedenken hoe je de mensen in de organisatie bewust maakt van een datalek .
- Om te bedenken welke preventieve en reactieve (noodvoorzieningen en het vervolg) maatregelen je in zo'n situatie neemt en of je daarbij advies nodig hebt .

IT solutions in green

De slottip:

Met deze tips is (samenvattend) geïnventariseerd:

- Welke persoonsgegevens er zijn.
- Wat met persoonsgegevens wordt gedaan.
- Of de verwerking passend is bij de gerechtvaardigde grondslag.
- Wie toegang hebben tot de persoonsgegevens.
- Hoe autorisaties zijn geregeld.
- Met welke externe partijen een verwerkersovereenkomst nodig is.
- Van welke technische inrichting er sprake is.
- Hoe het gedrag is van mensen in de omgang met persoonsgegevens.
- Hoe relaties geïnformeerd worden over de omgang met persoonsgegevens.
- Wie de interne contactpersoon is in geval het mis gaat door datalekken.

Het is een absolute aanbeveling om alle informatie die je nu hebt verzameld, te gaan delen met een expert. Dit te koppelen aan een “scan” die je meer inzicht geeft over waar de risico’s zich bevinden en wat je kunt ondernemen. Niet alleen in het kader van de AVG, maar uiteindelijk ook de bedrijfsrisco’s.

De slottip is het einde van de voorbereiding. De laatste tip bij het verzamelen van informatie, als afsluiter, is om te bepalen hoe je het vervolg verder wilt oppakken en wat en wie daarvoor nodig is.

We hopen dat we jullie hiermee een beetje op weg hebben geholpen in de voorbereiding.