Whitepaper

Gebruik de GDPR als onderscheidend vermogen

Learnings uit de praktijk

Tripolis Solutions

We deliver

Goed dat je deze whitepaper hebt gedownload.

Een bewijs dat de privacy van jouw leads, prospects en klanten net zo belangrijk is als voor ons.

Op het moment dat je deze whitepaper leest is het vijf voor twaalf: het is bijna zover dat de Wbp (Wet bescherming persoonsgegevens) en 'cookiewet' vervangen worden door de GDPR (General Data Protection Regulation). De GDPR is de Europese verordening, waarvan de AVG (Algemene Verordening Gegevensbescherming) een afgeleide is. Voor het gemak spreken we in deze whitepaper alleen over de GDPR.

Het is vijf voor twaalf

Als marketeer word je overspoeld met informatie over de nieuwe wetgeving. Je bent dan ook al bekend met dit onderwerp, maar mist wellicht concrete voorbeelden 'uit het veld' voor een laatste check. En inzicht wat je absoluut op orde moet hebben om geen boete te riskeren.

In deze whitepaper hebben we daarom de meest relevante informatie voor je verzameld over hoe je op 25 mei zo goed mogelijk op weg bent voor een GDPR-proof organisatie. Met veel praktische tips en learnings. Na het lezen van deze whitepaper weet je wat je te doen staat om de privacy van consumenten te waarborgen, volgens de richtlijnen van de Wet Autoriteit Persoonsgegevens.

Waarom wil Tripolis een bijdrage leveren aan dit onderwerp?

Tripolis wil een bijdrage leveren aan de discussie rondom de GDPR omdat het verantwoord omgaan met data voor ons vanzelfsprekend is. Hierdoor toon je immers respect naar je klanten. Omdat dit gegeven ons vanaf de start van onze oprichting bestaansrecht geeft, willen we, vooral nu het onderwerp zo actueel is, onze klanten helpen met tips om dit zo goed mogelijk te regelen.

Deze whitepaper is een initiatief van Tripolis en is mede mogelijk gemaakt door o.a. De Privacy Pro, 100% E-mail en Order2Cash.

Goed voorbereid op het GDPR tijdperk

Om niet te verdwalen in alle regelgeving van de GDPR hebben we een aantal partners/ organisaties gevraagd naar wat zij de meest opvallende artikelen vinden uit de nieuwe wet. Hoe hebben zij zich voorbereid? Wat zijn hun bevindingen tot nu toe? In deze whitepaper vind je hun learnings uit de praktijk. Doe er je voordeel mee!

In deze whitepaper:

- Wat is de GDPR?
- Wat zijn de vereisten?
- Impact van de GDPR op online marketing
- Impact van de GDPR op e-mailmarketing
- Learnings uit de praktijk, vanuit de verschillende rollen

Wie biedt je deze whitepaper aan?

Tripolis is opgericht in 1999 als een cross channel dialogue marketing platform voor e-mail, mobile en social marketing. Met andere woorden: wij zijn specialist in het aanbieden van e-mail en marketing technologie. Hierdoor helpen wij onze klanten de ervaring van hun klanten te verbeteren. We helpen klanten hun marketing processen te automatiseren en bij te blijven. Dit doen wij door het voor marketeers mogelijk te maken om met grote aantallen klanten tegelijk, maar toch individueel, te communiceren.

In het kort nog even het uitgangspunt en de hoofdlijnen van de GDPR op een rij.

Wat is de GDPR?

De GDPR is al op 25 mei 2016 gelanceerd, met de afspraak dat deze 2 jaar later officieel van kracht gaat. Dit om een overgangsperiode te creëren tussen de Wpb en de GDPR. Wat er globaal verandert is dat de nieuwe wet de privacyrechten van natuurlijke personen uitbreidt, dat organisaties die persoonsgegevens verzamelen meer verantwoordelijkheid nemen om zorgvuldig met die gegevens om te gaan, en dat toezichthouders mogelijkheden krijgen om boetes op te leggen bij overtreding van de wet. En deze boetes zijn fors: deze kunnen oplopen tot € 20.000.000 of 4 procent van de wereldwijde jaaromzet.

Voor jou als marketeer betekent deze wet dat je veel bewuster moet omgaan met persoonsgegevens. Zowel bij B2C als bij B2B.

Wat zijn de vereisten?

Om na 25 mei 2018 geen boete te riskeren, moet je als organisatie aan de volgende eisen voldoen:

1. Transparantie: maak duidelijk dat je gegevens verwerkt die je opvraagt, vraag hier duidelijk (ondubbelzinnig) toestemming voor en wijs iemand op zijn rechten.

2. Doelbinding: maak duidelijk waarvoor je die gegevens verzamelt en gebruik die gegevens ook niet voor iets anders.

3. Dataminimalisatie: vraag alléén die gegevens op, die je voor het aangegeven doel nodig hebt.

4. Beveiliging en opslagbeperking: zorg voor een goed beveiligde opslag van de gegevens. Hoe gevoeliger de gegevens, hoe hoger de beveiliging.

5. Privacy by design: besteed al bij de ontwikkeling van nieuwe producten en diensten aandacht aan privacy verhogende maatregelen.

6. Privacy by default: zorg ervoor dat je standaard alléén de gegevens verwerkt die noodzakelijk zijn voor het doel dat je wilt bereiken. Bijvoorbeeld door in een app niet om de locatie te vragen als dat niet nodig is. Of op je webformulier geen vakjes vooraf aan te vinken.

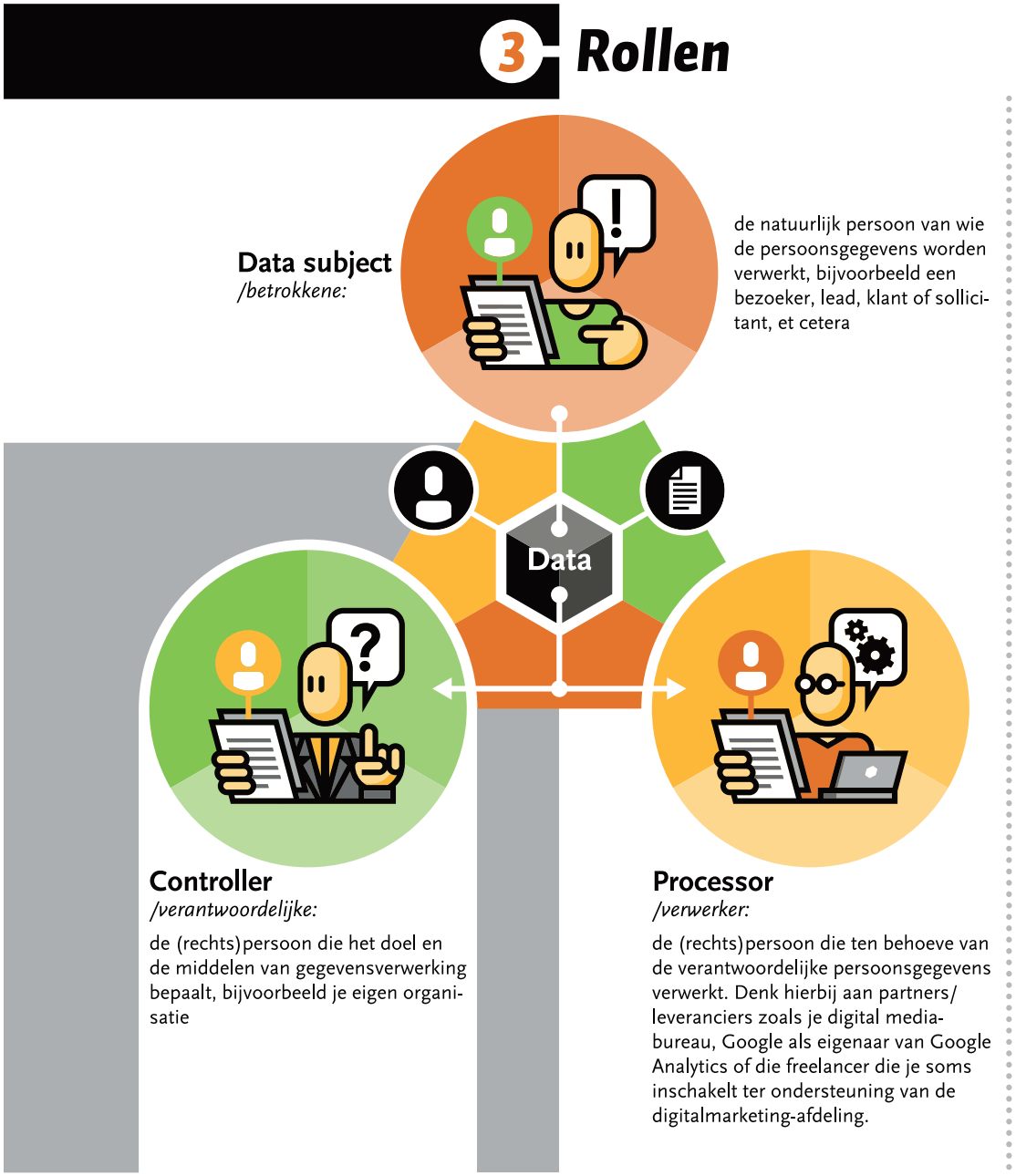
Tip: Zorg er verder voor dat gegevens altijd correct zijn, dat je gegevens niet langer bewaart dan nodig is en dat je te allen tijde kunt aantonen dat je aan de regels voldoet.

Welke rol in de keten?

Kijk ook goed naar welke rol jij hebt, of je organisatie heeft, bij de verwerking van gegevens:

- **Een 'data subject' of 'betrokkene':** personen van wie de gegevens worden verwerkt, denk aan een bezoeker, lead, klant of sollicitant.
- **De 'controller' of 'verantwoordelijke':** de rechtspersoon die bepaalt wat er met de opgevraagde gegevens gebeurt en hoe die gegevens worden opgevraagd, denk aan je eigen organisatie.
- **De 'processor' of 'verwerker':** rechtspersoon die (in opdracht) iets doet met de gegevens, denk daarbij ook aan een extern mediabureau of een freelancer.

In deze whitepaper laten we een aantal bedrijven aan het woord, die bij het verwerken van gegevens één van deze rollen vervult. Lees verder!



Impact van de GDPR op online marketing

Is online marketing een focuspunt in jouw werk als marketeer? Kijk dan goed naar de definitie van het begrip 'persoonsgegevens'. Deze is in de nieuwe wet flink aangescherpt. Er wordt onderscheid gemaakt tussen persoonsgegevens, pseudo-anonieme gegevens en anonieme gegevens. Dat betekent dat er vanaf 25 mei meer datatypen onder persoonsgegevens vallen.

Een kritische blik is nodig bij:

1. Formulieren op je website die vragen om NAW-gegevens.

Gegevens die hierop worden ingevuld, moeten versleuteld verzonden worden via https. Checkboxes mogen niet meer standaard aangevinkt zijn.

2. Privacy & cookiestatement.

Schrijf een privacyverklaring waar geen woordenboek bij nodig is om te snappen wat er staat.

Denk hierbij verder aan:

- **Opt-in en opt-out mogelijkheden:** geef duidelijk aan wat de bedoeling is en vraag om toestemming.

- **Samenwerking met derden:** wie zijn de andere 'verwerkers' van de ingevulde gegevens, wat doen zij met die gegevens en waarom doen ze dat?

- **Profilering:** geef aan waarom je profielen van bezoekers opbouwt en met welk doel, geef aan welke tools je hiervoor gebruikt, hoe die tools de cookies plaatsen én hoe een bezoeker die cookies ook weer kan verwijderen.

- **Recht tot inzage (recht op vergetelheid & dataportabiliteit):** maak het zo makkelijk mogelijk voor bezoekers om gegevens te (laten) wijzigen, te (laten) verwijderen of te ontvangen om ze aan een ander, soortgelijk bedrijf te kunnen overdragen.

- **Klacht indienen:** geef aan hoe en waar bezoekers terechtkunnen voor het indienen van een klacht (Autoriteit Persoonsgegevens).

- **Privacy verantwoordelijke:** noem naast de bedrijfsgegevens ook de naam van de persoon die zich namens de organisatie bezighoudt met de bescherming van de persoonsgegevens.

Impact van de GDPR op e-mailmarketing

Over de veranderingen voor e-mail opt-in wordt veel gespeculeerd. Het vragen om opt-in voor het versturen van e-mail met sales doeleinden valt onder de Telecommunicatiewet. De toezichthouder van deze wet is de Autoriteit Consument en Markt. Aan deze wet verandert (voorlopig) niks.

Waar de GDPR wél invloed op heeft, is de manier waarop toestemming gegeven wordt. Is het duidelijk genoeg voor de bezoeker waar hij 'ja' tegen zegt (Specifiek)? Staan er geen standaard vinkjes in de checkboxes (Vrij)? Weet de bezoeker hoe vaak hij een e-mail kan verwachten en wat de aard van deze e-mails is (Op informatie berustend)? Kun je als organisatie bewijzen dat je toestemming hebt gekregen voor dat wat je met de gegevens doet (Ondubbelzinnig)?

Vier snelle tips voor de online marketeer:

1. Inventariseer:

- **Welke data je verzamelt.**
- **Van wie je dat doet.**
- **Met welk specifiek doel.**
- **Welke tools en 'verwerkers' hierbij betrokken zijn.**
- **Hoe je data verwerkt en opslaat.**

2. Maak gebruik van https-encryptie, zeker bij formulieren.

3. Stel verwerkersovereenkomsten op voor partners en leveranciers in eenvoudig taalgebruik.

4. Update je cookiepolicy en privacy statement, in eenvoudig taalgebruik.

Rol Accell in de keten: Controller

Learnings: 100% E-mail

Lees meer over de uitdaging van Accell bij de implementatie van de GDPR. En hoe Ruud Ouweneel & Katja Graaf van 100% E-mail dit hebben opgepakt.

Uitdagingen van Accel Nederland

Over Accell Nederland

Accell Nederland is marktleider in het midden- en hogere segment van fietsen, fietsonderdelen en fietsaccessoires. In Nederland vallen merken als Batavus, Sparta, Koga en Loekie onder dit label.

Waar loopt Accell Nederland tegenaan?

Accell bestaat uit meerdere bedrijven die bij elkaar zijn gevoegd. Hierdoor maakt Accell gebruik van verschillende E-mail Service Providers. Hun wens: één centraal e-mailmarketing systeem én klaar zijn voor de GDPR.

Aanpak

100% E-mail heeft alle databronnen en de opt-in en opt-out processen (de datastromen) onderzocht. Op basis daarvan is een concrete actielijst opgesteld.

"Zorg ervoor dat je zo snel mogelijk een projectteam samenstelt van diverse betrokkenen uit de organisatie. Zo creëer je een gezamenlijke organisatiebewustzijn in de omgang met persoonsgegevens." – Ruud Ouweneel

Learnings

1. Wel of geen rechtspersoon?

Accell communiceert heel veel met dealers (de rijwielhandelaren) via e-mail. Zijn die dealers nu wel of geen rechtspersonen? En heb je dan wel of geen toestemming nodig voor het verzamelen van gegevens? Hiervoor maak je dus onderscheid tussen natuurlijke personen en rechtspersonen. En als het om een natuurlijk persoon gaat, dan gaat het per definitie over persoonsgegevens. Maar ook een bedrijfsemailadres met een persoonlijke naam er in, is een natuurlijk persoon. Wees je hier goed van bewust.

2. De reikwijdte is breder geworden.

Voor 'remarketing' of retargeting van e-mailcampagnes met een display advertising geldt dat je te maken hebt met cookies. Hiervoor maak je gebruik van setting pixels. Zo'n cookie bestaat ook weer uit persoonsgegevens, afkomstig van IP-adressen. Wat dat betreft is de reikwijdte van de nieuwe wet veel breder geworden.

Let verder goed op je cookiestatement en cookiemelding. Cookie walls (akkoord of niet akkoord gaan) mogen bijvoorbeeld niet meer. Je moet nu ook een werkende site aanbieden als iemand niet akkoord gaat met je cookiestatement. Dat betekent dat je een cookie oplossing nodig hebt, waarbij websitebezoekers meer gedifferentieerd hun toestemming kunnen geven. Daar zijn software oplossingen voor; dit hoef je niet allemaal zelf te bouwen.

3. Weet waarvoor je gegevens verzamelt.
Kijk op welke plekken je persoonsgegevens verzamelt en met welk doel. Doelen kunnen zijn: het leveren van producten, uitleg geven over je producten of een nieuwsbrief versturen.

4. Wees scherp op je e-mailmarketing.
Leg vast op welk moment je toestemming hebt gekregen voor het gebruik van gegevens en op welke manier: via een pop-up op de website of tijdens een gesprek op een beurs? En waar heb je exact toestemming voor gekregen? De wet vraagt dat nu veel meer in detail.

Tip: grijp dit moment aan om je e-mailmarkting-beleid opnieuw onder de loep te nemen. Kijk waar je onderdelen van je organisatie kunt vernieuwen. Kun je je mailing bijvoorbeeld differentiëren, waardoor je voor de ontvanger meer relevantie toevoegt? Nog een voordeel: iemand die zich uitschrijft kan zich zo ook voor maar één onderdeel of onderwerp uitschrijven.

5. Kijk naar je webformulieren.
Denk aan dataminimalisatie: je mag alleen die gegevens uitvragen die je nodig hebt. Als je een nieuwsbrief wilt versturen, heb je niks aan iemands geboortedatum. Tenzij je op iemands verjaardag iets leuks wilt doen. Vraag in elk geval nooit teveel uit. En verwijs altijd naar je privacy statement. Geef daarop aan wat het doel is van de verwerking. Dat hoef je dus niet in je webformulier op te nemen.

Conclusie

Alle informatie over de nieuwe wet is beschikbaar. Maar haal je specialistische kennis in huis, dan is de kans groter dat het beter, sneller en efficiënter geregeld is. Vaak is het ook wel prettig om iemand van buitenaf naar de situatie te laten kijken. Bij Accell heeft dat goed uitgepakt.

Rol Order2Cash in de keten: Verwerker (processor).

Learnings: Order2Cash

Lees meer over de learnings van Marco Eeman: eigenaar en CTO van Order2Cash, en partner van Tripolis.

Over Order2Cash

Specialiteit van Order2Cash is het veilig opslaan, bewaren en distribueren van documenten. Als geavanceerde e-mailmethoden nodig zijn, met meer kennis over het afleveren via de mail, dan schakelt Order2Cash Tripolis in.

Wat is de taak van Order2Cash?

Order2Cash krijgt van klanten gegevens, waarmee onder meer digitale facturen kunnen worden gemaakt en gemaild namens deze klanten. Order2Cash heeft in de rol van verwerker dus inzage in de gegevens voor het afleveren, denk aan e-mailadressen, maar verandert niks aan zo'n adres zelf.
De controller (of verwerkingsverantwoordelijke) moet ervoor zorgen dat de inhoud van de gestuurde gegevens klopt, en dat deze verwerkt mag worden.
In het geval van Order2Cash is de controller de verzekeringsmaatschappij of de autoleasemaatschappij die Order2Cash de gegevens stuurt. De controller mag gegevens alleen doorgeven aan een verwerker die "passende technische en organisatorische maatregelen" voor de verwerking kan leveren. Aan Order2Cash dus de taak om GDPR-compliant te zijn als verwerker, maar ook te zorgen dat subverwerkers met toegang tot de gegevens compliant zijn.

Aanpak

Order2Cash heeft al een goed overzicht van wie er allemaal in de keten zit. Voor Order2Cash is dit het moment om van alle geschakelde bedrijven te onderzoeken hoe compliant zij zijn en of (eventuele) certificeringen (nog) goed op elkaar aansluiten. Deze 'keten van vertrouwen' is voor verwerkers heel belangrijk.

Hiervoor heeft Order2Cash eerst de eigen rol in de keten vastgesteld. Op basis van deze rol heeft Order2Cash de meest belangrijke maatregelen uit de wetgeving gedestilleerd. Hiervoor is voldoende publiekelijke informatie beschikbaar. Daarna is in kaart gebracht voor welke maatregelen al een oplossing bestaat.

Tip: kijk of je de oplossingen die je al hebt voor het beschermen van persoonsgegevens ook kunt bewijzen, of dat je kunt aangeven hoe je tot die oplossing gekomen bent. Nodig hiervoor eventueel een auditor uit. Order2Cash laat bijvoorbeeld de ISAE 3402-audit uitvoeren.

"Is je dienstverlening van hoge kwaliteit, dan mag je er vanuit gaan dat je aan veel toekomstige regels voldoet. Wat betekent dat je je minder druk hoeft te maken om 25 mei dan je denkt."

Learnings

1. Zorg dat je geen bijvangst hebt.

Spreek met je klant af dat die jou geen gevoelige of bijzondere gegevens stuurt tenzij het nodig is en dit apart is afgesproken. Order2Cash verwerkt facturen en verzekeringspolissen. Op een factuur hoeft bijvoorbeeld geen BSN te staan. Als bijzondere of gevoelige gegevens niet worden opgestuurd, hoef je er ook niet over na te denken en er geen passende maatregelen voor te nemen.

2. Stel met elke klant een overeenkomst op.

Zorg ervoor dat voor elke dienst, waarbij je persoonsgegevens verwerkt voor een klant, een overeenkomst met verwerkingsovereenkomst is getekend. Zonder geldige overeenkomst, of als je andere dingen doet met de ontvangen persoonsgegevens dan overeengekomen, word je onder de GDPR gezien als verwerkingsverantwoordelijke met daarbij horende plichten. Dus let op je rol. Kijk ook of je overeenkomst nog wel geldig is; het kan zijn dat je overeenkomst van rechtswege afloopt.

3. Stel met elke subbewerker een overeenkomst op.

Zorg ervoor dat je afspraken met je subbewerkers passen binnen de afspraken met je klanten of andersom. Als je bijvoorbeeld met je klant afspreekt dat je een datalek binnen 24 uur meldt, moet je met je subbewerker afspreken dat die zijn datalekken in minder dan 24 uur aan jou doorgeeft. Kom alleen service levels met je klant overeen die je subverwerker kan nakomen.

4. Zorg dat je register op orde is.

Onder de GDPR moeten verwerkers en verwerkingsverantwoordelijken een register bijhouden waarin alle verwerkingen met persoonsgegevens staan. Meestal ben je als dienstverlener zowel verwerker (voor de gegevens die je voor je klanten verwerkt) als verwerkingsverantwoordelijke (voor bijvoorbeeld je personeelsadministratie).

Conclusie

Bij de implementatie van deze wet gaat het óók om de ketensamenwerking, waarin iedereen z'n eigen verantwoordelijkheid heeft. Het is dus belangrijk dat élke schakel in de keten compliant is.

Learnings: De Privacy Pro

Lees meer over de aanbevelingen van John Yonce, Data Protection Officer en oprichter van De Privacy Pro.

Over de Privacy Pro

John Yonce geeft als de Privacy Pro adviezen aan bedrijven die met persoonsgegevens werken. John heeft 4 jaar in de IT gewerkt en is van huis uit jurist.

Wat is de uitdaging voor bedrijven in aanloop naar de GDPR?

Vanaf Q4-2016 naar Q4-2017 is het aantal datalekmeldingen verdubbeld. Deze stijgende lijn laat zien dat de schaamte over het niet volledig op orde hebben van gegevensbescherming afneemt. Het kan ook zijn dat meer bedrijven bekend zijn met de Meldplicht in de Wet Bescherming Persoonsgegevens. Toch is het nog steeds een pijnpunt dat bedrijven open en eerlijk moeten zijn over hun omgang met persoonsgegevens.

Aanpak

Met certificeringen als ISO-9001 (management kwaliteitssystemen) en ISO-27001 (informatiebeveiliging) kun je aantonen dat je als bedrijf gereguleerd bent, en dus klaar bent voor de GDPR. Ook Tripolis heeft deze certificeringen. Al sinds 2007.

Learnings

1. Stel een verzoekprocedure op.
Naar aanleiding van de GDPR zijn ook consumenten ondervraagd. Uit dat onderzoek blijkt dat 80% van de mensen gebruik zullen maken van hun rechten onder de nieuwe privacy wetgeving. Bereid je als bedrijf daarom voor op verzoeken met betrekking tot verstrekte persoonsgegevens. De wet schrijft voor dat je binnen 4 weken moet reageren. Zie dit als een stukje klantvriendelijkheid, dan voelt de hele organisatie zich meer verantwoordelijk.

2. Maak opt-in mogelijkheden steeds specifieker.
Het moet net zo makkelijk zijn om ergens 'ja' op te zeggen als om 'nee' te zeggen. Ter illustratie: bij de aanschaf van een Apple-product teken je een gebruikersovereenkomst. Apple mag op dat moment dan niet óók toestemming vragen om je gegevens te gebruiken voor marketingdoeleinden. Dit moet voor de GDPR uit elkaar getrokken worden. Dit heet ook wel "layered consent".

3. Doe aan 'datamappen' en maak een verwerkingenregister. Wat voor gegevens gebruik je? Met welk doel? Welke partijen hebben hierin nog meer inzage? Breng deze uitkomsten onder in een verwerkingsregister dat je kunt overhandigen als de Autoriteit Persoonsgegevens daarom vraagt.

4. Leg de informatie uit punt 3 vast in een privacy statement (een externe verklaring – voor klanten, patiënten of burgers) en een privacy policy (een intern beleid – voor werknemers).

"Zie investeren in informatiebeveiliging als een vorm van marketing: Bij ons zijn je gegevens wél veilig"

5. Stel bewaartermijnen op.

Zorg dat je bewijs hebt dat je rechtmatig, eerlijk en transparant met gegevens omgaat. Dat het verzamelen van gegevens tot het hoognodige beperkt blijft en dat je gegevens up to date houdt. Archiveer persoonsgegevens die niet meer nodig zijn en verwijder deze als de bewaartermijn voorbij is.

6. Neem technische en organisatorische maatregelen.

Voor technische maatregelen kun je denken aan een goede firewall en virusscanner en goede sloten. En organisatorische maatregelen: creëer awareness, organiseer sessies.

Tip: Creëer awareness voor social engineering: dit gaat over mensen die proberen van buitenaf informatie te stelen, door zich voor te doen als iemand anders. En awareness voor phishing.

7. Bekijk de checklist van de Information Commision Office.

Deze lijst is opgesplitst in verwerkers en verwerkingsverantwoordelijken en biedt kleine organisaties houvast bij het voldoen aan de GDPR. Het moet allemaal passend voor de organisatie zijn, daarvoor vind je hier veel handige tips.

Conclusie

De Autoriteit Persoonsgegevens wil dat je als organisatie bewuster omgaat met data. Als je meewerkt en je geeft aan dat je wilt verbeteren, dat je zaken zult aanscherpen en dat je ergens naartoe onderweg bent, dan helpt dat bij een eventueel onderzoek mocht er onverhoopt iets foutgaan in de organisatie. En: reageer altijd adequaat en snel op klachten over persoonsgegevens.

Rol van Tripolis in de keten: Verwerker (processor).

Learnings: Tripolis

Lees meer over de aanbevelingen van Remco Groen: COO van Tripolis.

"De nieuwe wetgeving biedt vooral kansen"

Wat is de belangrijkste taak van Tripolis in aanloop naar de GDPR?

De taak van Tripolis is enerzijds om voldoende technische en organisatorische maatregelen te nemen voor veilige dataverwerking. En anderzijds om het voor gebruikers zo gemakkelijk mogelijk te maken om aan de nieuwe wet te voldoen. Daarbij beoordeelt Tripolis nadrukkelijk niet of de verzamelde gegevens relevant zijn voor het doel.

Aanpak

Genoemde maatregelen zijn door Tripolis sinds 2007 al grotendeels door hun ISO-systeem geborgd. In het adviseren van klanten speelt deze whitepaper een rol.

Learnings

1. Onderzoek eerst: wat hebben we al aan data liggen?

Welke data heb je, waarvoor en wanneer wordt deze verwijderd?

2. Toets bestaande overeenkomsten.

Stel met alle bestaande gebruikers vast of er een juiste overeenkomst onder de geleverde dienst ligt. Dit is een gedeelde verantwoordelijkheid voor zowel de verwerker als de controller. Juridische afspraken moeten kraakhelder zijn en goed worden vastgelegd.

Tip: leg een register aan van alle bestaande gebruikers en overeenkomsten. Toets met name bij oudere overeenkomsten of die nog voldoen.

3. Nieuwe wetgeving biedt vooral kansen.

Dit is het moment om je positief te onderscheiden. Verplaats je zoveel mogelijk in je klant of degene met wie je communiceert en bedenk waar jij jezelf prettig bij zou voelen bij het verwerken van data. Doe dit bij al je processen en je krijgt meer tevreden klanten.

4. Wees open en eerlijk en stel je als organisatie kwetsbaar op.

Als verwerker moet Tripolis het mogelijk maken om aan verzoeken van klanten te voldoen, die zich beroepen op hun recht op inzage of recht op vergetelheid. De partners van Tripolis moeten hier als eerste op reageren, vervolgens zorgt Tripolis ervoor dat die data ook daadwerkelijk verwijderd wordt. Tripolis zal dit nooit direct doen, tenzij de termijn overschreden dreigt te worden. Organisaties moeten binnen 4 tot 8 weken reageren.

Tip: het risico bestaat dat verwijderde gegevens na een back up automatisch weer teruggeplaatst worden.

Tripolis houdt daarom een register bij van alle 'verwijderverzoeken' die binnenkomen. Dit register is gemakkelijk te raadplegen als er een calamiteit heeft plaatsgevonden waarvoor een back up gemaakt moet worden.

5. Denk bij elke nieuwe start aan de GDPR.

Bezig met de lancering van een nieuw product? Denk dan bij de start al aan hoe je de privacybescherming hebt georganiseerd. Zoals omschreven in de 'Privacy by default' en 'Privacy by design'. Voorheen kwamen deze punten als laatste aan bod. Nu moeten dit één van de eerste checkboxes zijn op een projectpuntenlijst.

6. Kijk kritisch naar met welke partij je in zee gaat.

Doe je wel zaken met een partij die aan de GDPR voldoet? Je kunt niet meer klakkeloos elk online tooltje gebruiken voor je marketingactiviteiten. Staat je data bijvoorbeeld wel opgeslagen in Europa? En heb je een gedegen verwerkingsovereenkomst vastgesteld? Grote bedrijven krijgen zo een vaste set van voorkeursleveranciers met wie zij zaken doen. Tripolis is zo'n voorkeursleverancier.

7. Maak een onderscheid tussen de opt-in en de dataverwerking.

De e-mail opt-in is onderdeel van de Telecommunicatiewet. Dat doen veel bedrijven al goed.

De opt-in is een pagina waarop bezoekers kunnen aangeven dat ze een nieuwsbrief willen ontvangen. Vraag je dan ook nog om aanvullende gegevens, zoals voornaam en woonplaats, dan kom je op het terrein van de GDPR.

Organisaties die hun opt-in en dubbele opt-in inderdaad al goed geregeld hebben, zullen weinig problemen ondervinden. Maar: wat ga je met die gegevens doen? Ga je profileren, segmenteren: hierover moet je mensen informeren. Dit betekent dat je mensen opnieuw om toestemming moet vragen.

Tip: De DDMA, brancheverenigingvoor data en marketing, heeft sinds vorig jaar heel veel juridische informatie verstrekt over de implementatie van de GDPR. Dit is vooral voor kleinere bedrijven interessant die zelf geen jurist in huis hebben.

Conclusie

Als je met een goede partij samenwerkt, komt het in orde. Voor Tripolis is dataveiligheid een tweede natuur. Wat inhoudt dat bij Tripolis elke (nieuwe) medewerker wordt bijgepraat en opgeleid in awareness. Dit is onderdeel van het ISO-systeem. Daarnaast organiseert Tripolis regelmatig awareness sessies. Want hoe mooi je het technisch ook hebt geregeld, de zwakste schakel is vaak een persoon.

Vragen naar aanleiding van deze whitepaper? Neem contact op!

Bram Smits | CEO

Tripolis B.V.

Web: http://www.tripolis.com

Mobile: +31 (0) 6 82 77 66 16

E-mail: bsmits@tripolis.com

Tripolis is een ISO 9001:2015 and ISO/IEC 27001:2013 gecertificeerd bedrijf.