De nieuwe Europese Privacywetgeving: kostenpost of concurrentievoordeel?

Zo haalt u voordeel uit de AVG

Auteurs:
Kees Gordijn, CFO Capabel
Hans Kortekaas, ID Control
Rembrandt de Haan, ID Control

De nieuwe Europese Privacywetgeving: kostenpost of concurrentievoordeel?

Inleiding

“Ernstig beveiligingslek in veelgebruikte wifi-beveiliging gevonden.”
“Dataverwerking Windows 10 in strijd met Nederlandse wet.”
“Hack in Yahoo in 2013 trof 3 miljard accounts.”
“Equifax opnieuw slachtoffer van cyberaanval.”
“GPS-horloges kinderen zeer slecht beveiligd.”
(bron: Nu.nl)

Zomaar een paar berichten die de afgelopen maanden in het nieuws verschenen. Stuk voor stuk voorbeelden van bewuste of onbewuste schendingen van privacy. De meeste daarvan betreffen beveiligingsissues gerelateerd aan het internet.

Op 25 mei 2018 eindigt de overgangsperiode van de Wet bescherming persoonsgegevens (Wbp) naar de Algemene verordening gegevensbescherming (AVG). De AVG treedt dan definitief in werking en zal vanaf die datum ook worden gehandhaafd door alle Europese privacytoezichthouders. Voldoet uw onderneming niet aan deze nieuwe privacywetgeving, dan riskeert u in geval van datalekken hoge boetes tot maximaal 20 miljoen euro of 4% van uw omzet. Reden genoeg om dit onderwerp met hoge prioriteit op de agenda te zetten. Of eigenlijk had u dat al moeten doen.

Bij de woorden ‘privacy’ en ‘bescherming van persoonsgegevens’ denkt u als MKB-ondernemer waarschijnlijk direct aan correct omgaan met persoonlijke gegevens die u via uw website binnenkrijgt. En beveiliging van uw netwerk tegen kwaadwillenden. Niet aan een e-mailbericht dat u per ongeluk aan de verkeerde persoon stuurt met grote gevolgen, of uw USB-stick met bedrijfsgevoelige informatie die onbewaakt op uw bureau ligt.

In deze whitepaper vertellen we u meer over de consequenties van de invoering van de AVG op juridisch, organisatorisch en technisch gebied voor het MKB. Aan de hand van voorbeelden uit de dagelijkse praktijk maken we u bewust van de impact die deze nieuwe wetgeving heeft op uw bedrijfsvoering. En we laten u zien hoe u voordeel kunt behalen uit de nieuwe privacywetgeving door verder te kijken dan de verplichtingen en de kosten.

De nieuwe Europese Privacywetgeving: kostenpost of concurrentievoordeel?

Inhoud

De nieuwe Europese Privacywetgeving: kostenpost of concurrentievoordeel?

1. Veel bedreigingen, weinig kennis

Het aantal bedreigingen van de privacy neemt enorm toe, maar de kennis bij het MKB is beperkt. De meeste organisaties hebben moeite om te begrijpen wat de privacywetgeving inhoudt. Er zijn veel beschrijvingen van de wet, maar de meeste zijn zeer wollig. En praktische toepassingen voor ondernemingen om hun business snel aan te passen naar de nieuwe privacywetgeving ontbreken.

1.1. Het yin en yang van internet

In elk goeds zit iets kwaads. De technologische ontwikkelingen hebben de laatste jaren een enorme vlucht genomen. Aan de ene kant ontstaan daardoor talloze nieuwe mogelijkheden. Maar aan de andere kant brengt dit ook vele nieuwe bedreigingen met zich mee. Anders gezegd: op het internet is iedereen een zittend eendje waarop een jager vanuit een hutje kan schieten.

1.2. Bekendheid van securitydreigingen

Welke securitydreigingen zijn het meest bekend bij organisaties en particulieren?

- Phishing (60%)
- Malware (52%)
- Social engineering / spoofing (41%)
- Hackpogingen (36%)
- Verlies mobiele apparaten (34%)
- Werknemersdiefstal (16%)
- SQL Injecties (15%)
- Watering hole (8%)
- Man-in-the-middle attacks (7%)

(bron: State of Cyber Security, ISACA 2016)

1.3. Voorbeelden van malafide internetpraktijken

Phishing

U hebt ze vast wel eens gezien, e-mailberichten die afkomstig lijken te zijn van officiële instanties. De strekking van deze e-mails is altijd hetzelfde: “Klik op deze link om …”. Klikt u op de link, dan komt u op een betrouwbaar uitziende webpagina, zogenaamd op de website van de instantie. Hier wordt u gevraagd in te loggen of bepaalde persoonlijke gegevens in te vullen.

CEO e-mail fraude

Een minder bekende maar steeds vaker voorkomende vorm van phishing is als u een e-mail krijgt met een betaalverzoek, zogenaamd verstuurd vanuit het management. Niets is echter minder waar: het e-mailadres is via een handige truc ‘gestolen’ (gespoofd) door internetcriminelen en wordt nu gebruikt om u geld te ontfutselen.

Malware

U installeert een programma op uw computer, opent een bijlage in een e-mail of downloadt een game, film of foto's. En ineens gebeuren er rare dingen: bekenden ontvangen vreemde berichten uit uw naam. Of op uw computer verschijnt een mededeling dat hij vergrendeld is en alleen kan worden ontgrendeld door geld te betalen. Wat is er aan de hand? Ongemerkt is er malware meegekomen, ingenieuze bestandjes die uw privacy schenden, schade aan uw computer toebrengen of de normale werking van uw computer verstoren.

1.4. "Maar wij hebben toch niets te verbergen?"

Nu denkt u vast: waarom zouden ze mijn computer of mijn netwerk willen hacken, wij hebben toch niets te verbergen? Maar elke computer is interessant voor hackers. Is het niet vanwege uw bedrijfsgevoelige informatie, dan kan uw computer bijvoorbeeld wel worden ingezet bij een DDoS-aanval of voor de verdere verspreiding van malware.

Er staat meer online dan u denkt

Via de diverse media en apps is er over u vaak meer online te vinden dan u vermoedt. NAW-gegevens, gebruikersnamen en wachtwoorden, IP-adressen, ja zelfs creditcardgegevens blijken online te staan. Natuurlijk zet u zelf wellicht ook dingen online via bekende kanalen als website, Facebook, LinkedIn of Marktplaats. Maar vaak geeft u zonder dat u het weet meer prijs dan u lief is. Omdat u via een onveilig openbaar netwerk gebruikmaakt van het internet. Omdat u wordt gefopt door een betrouwbaar uitziende e-mail die afkomstig lijkt van een officiële instantie. Of omdat u online alles wel goed heb beveiligd, maar er fysieke datalekkage plaatsvindt: uw smartphone kwijtgeraakt, uw laptop gestolen.

Eye-opener: openbare wifi's, een walhalla voor hackers

Bijna iedereen doet het: in de trein, op het vliegveld, tijdens het lunchen even via de openbare wifi het internet op. Even de social media checken, een e-mail beantwoorden, een betaling doen of appen met collega's of vrienden. Heel handig. Maar ook heel gevaarlijk. Een slimme hacker kan uw mobiele apparaat eenvoudig om de tuin leiden en zonder dat u het doorhebt doorsturen naar een eigen netwerk. Met alle veiligheidsrisico's van dien. Een walhalla voor hackers dus!

2. Algemene verordening gegevensbescherming (AVG)

Op 25 mei 2018 eindigt de overgangsperiode van de Wet bescherming persoonsgegevens (Wbp) naar de *Algemene verordening gegevensbescherming (AVG)* – of in het Engels *General Data Protection Regulation (GDPR)*. De AVG treedt dan definitief in werking en zal vanaf die datum ook worden gehandhaafd. Voldoet u als ondernemer niet aan deze nieuwe privacywetgeving, dan riskeert u in geval van datalekken hoge boetes tot maximaal 20 miljoen euro of 4% van uw omzet.
Is uw onderneming al voorbereid op de AVG?

2.1. Wat verandert er door de inwerkingtreding van de AVG?

De AVG zorgt onder meer voor:

- Versterking en uitbreiding van privacyrechten
- Meer verantwoordelijkheden voor organisaties
- Handhaving: met deze Europese verordening wordt een speelveld gecreëerd waarbij het niet meer mogelijk is dat binnen de EU geconcurreerd wordt op privacybescherming.

2.2. Wat betekent de invoering van de AVG voor u?

Verantwoordingsplicht: u moet met documentatie kunnen aantonen dat u de juiste organisatorische en technische maatregelen heeft genomen om aan de AVG te voldoen.

Documentatieplicht verwerking persoonsgegevens: u moet kunnen bewijzen dat u geldige toestemming hebt gekregen voor het verwerken van persoonsgegevens; deze toestemming moet op eenvoudige wijze weer kunnen worden ingetrokken.

Rechten van betrokkenen: toegang en overdraagbaarheid:

- *recht van inzage*: betrokkenen hebben het recht om in te zien welke persoonsgegevens u hebt opgeslagen dan wel verwerkt.
- *recht op correctie en verwijdering*: betrokkenen hebben het recht om persoonsgegevens te laten aanpassen of verwijderen. Deze aanpassing of verwijdering moet ook worden doorgegeven aan andere organisaties die deze gegevens van u hebben ontvangen.
- *recht op dataportabiliteit*: betrokkenen hebben het recht om van uw organisatie persoonsgegevens in een standaardformaat te ontvangen.

Privacy by default: technische en organisatorische maatregelen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken. Met als doel *dataminimalisatie*: niet meer informatie vragen dan nodig is voor het specifieke doel, en deze informatie ook niet langer bewaren dan nodig na het bereiken van dit doel.

Privacy by design: houd bij het ontwerpen van uw producten en diensten al rekening met een correcte verwerking van de privacygegevens. Denk bij voorbaat al na hoe de privacy gewaarborgd wordt. Bijvoorbeeld Windows 10 stuurt al uw zoekopdrachten naar Microsoft.

Meldplicht datalekken: een datalek moet u voortaan binnen 72 uur melden bij de Autoriteit Persoonsregistratie (AP) als u:

- uw persoonsgegevens verwerkt
- u verantwoordelijk bent voor deze verwerking
- u niet uitgezonderd bent van de wet
- er sprake is van een datalek in de zin van de wet.

Functionaris voor gegevensbescherming: een privacy officer aanstellen is verplicht voor:

- overheden en publieke organisaties,
- organisaties die op grote schaal individuen observeren of volgen
- organisaties die op grote schaal bijzondere persoonsgegevens verwerken, bijvoorbeeld over iemands gezondheid, ras, politieke opvatting, geloofsovertuiging of strafrechtelijk verleden.

Verwerkersovereenkomsten: als u bewerking van persoonlijke gegevens uitbesteedt aan derden, moet u met hen een deugdelijke overeenkomst sluiten waarin wordt vastgelegd:

- met welk doel de gegevensverwerking plaatsvindt
- welke persoonsgegevens verwerkt worden
- welke betrokkenen toegang hebben tot deze gegevens
- hoe deze gegevens passend beveiligd worden
- door wie en wanneer er audits uitgevoerd worden
- hoe de gegevens na afloop vernietigd worden of teruggeleverd aan de verantwoordelijke.

2.3. Uitwisseling van gegevens tussen Europa en de VS: het Privacy Shield

De AVG / GDPR geldt alleen voor gegevensbescherming binnen de EU. Daarnaast is sinds juli 2016 het Privacy Shield van toepassing, afgesloten tussen de VS en de EU. Dit privacyschild heeft als doel bij uitwisseling van persoonsgegevens met de VS een passend beschermingsniveau te bieden. Elke organisatie in de VS die gecertificeerd is bij het privacyschild, heeft een passend beschermingsniveau. Organisaties mogen vanuit Europa persoonsgegevens doorgeven naar deze organisaties in de VS.

3. Best practices en bespiegelingen

3.1. Waarom is die privacywetgeving eigenlijk nodig?

De media staan tegenwoordig bol van berichten over cybercriminaliteit en datalekken. Van het bedrijf van de buurman tot grote toonaangevende organisaties die hun security niet op orde hebben. Waar gaat het mis?

Onze constatering is dat veel bedrijven zich niet realiseren welke risico's ze lopen. Of ze weten het wel maar hebben simpelweg niet de kennis of de tijd om zich er goed in te verdiepen en accurate oplossingen te implementeren. Internetcriminelen maken daarvan dankbaar misbruik. De keten van beveiliging is zo sterk als de zwakste schakel en een veiligheidslek kan tot aanzienlijke schade en hoge onvoorziene kosten leiden.

Een paar recente voorbeelden van internetschandalen *(bron: Nu.nl):*

- **Een Amerikaans creditcardschandaal bij Equifax**
  Het creditcardbedrijf Equifax werd in mei 2017 gehackt, waarbij criminelen toegang kregen tot de gegevens van 143 miljoen Amerikanen. Dit werd in juli pas ontdekt. In oktober 2017 werden zij opnieuw de dupe van een cyberaanval.
- **Russische spionage via antivirus-software Kaspersky**
  Kaspersky, een Russisch antivirusprogramma, zorgde dat een subcontractor van de NSA zonder het te weten data heeft verstuurd naar Rusland. Dit werd ontdekt door Israëlische staatshackers.
- **Wereldwijde e-mailserver Deloitte gehackt**
  De wereldwijde e-mailserver van de cybersecuritytak van Deloitte werd een tijd geleden gehackt. Bijna elke organisatie heeft een volledig onversleutelde e-mailserver. Een hacker die de e-mail-server overneemt, kan vaak weer toegang krijgen tot gevoelige persoonsgegevens en andere systemen.

3.2. De ID Control AVG Compliancy driehoek

Om uw organisatie aan te passen naar de nieuwe privacywetgeving moet de zogenaamde AVG Compliancy driehoek worden ingevuld. Dit integrale model, gecreëerd door ID Control, geeft u een goede basis om te voldoen aan de AVG. Een betaalbaar en behapbaar model voor zowel het MKB als grote organisaties.

De ID Control AVG Compliancy driehoek omvat:

- juridische maatregelen
- organisatorische maatregelen
- technische maatregelen.

Aangezien de implementatie van de GDPR / AVG zeer veelomvattend is en bovendien sterk afhankelijk is van de aard van uw bedrijf, is het onmogelijk om alle aspecten van dit model in deze whitepaper uit te werken. Daarom behandelen wij op hoofdlijnen de belangrijkste maatregelen en aandachtspunten.

3.3. Juridische maatregelen

Privacy- & security (normen) kader

Privacy is maar een klein onderdeel van de door security te verdedigen belangen. Wat te denken van het ongestoord gebruiken van de ICT-systemen? Of het beschermen van niet-persoonlijke bedrijfsgeheimen? Waar bedrijven zelf verantwoordelijk zijn voor het beschermen van hun gevoelige gegevens, is de Europese wetgever opgekomen voor de bescherming van de privacy van de persoon.

Verwerkingsovereenkomst

Vrijwel alle toepassingen van uw onderneming draaien in een datacentrum of in uw eigen serverruimte. Uw leverancier heeft vaak dus toegang tot al die data. Verder werkt u wellicht samen met derde partijen die in uw opdracht persoonsgegevens verwerken. In beide gevallen hebt u een verwerkers-overeenkomst nodig waarin dit waterdicht wordt afgesloten.

Documentatieplicht

Alle organisaties zijn straks verplicht om aan de toezichthouder, de Autoriteit Persoonsgegevens, te kunnen laten zien dat ze “privacy (AVG) compliant” zijn. Uw organisatie moet met documenten aantonen dat u passende maatregelen hebt genomen. Belangrijk hierbij zijn een bedrijfsbreed informatiebeveiligingsbeleid met aandacht voor de technische kant (bijvoorbeeld backup & restore plan,

identity & access management) maar ook de organisatorische (mens)kant van de risicobeheersing (bijvoorbeeld security awareness, incident response procedure, en Bring Your Own Device beleid).
Deze registratie- en documentatieplicht geldt dus ook voor uw personeelsadministratie en klanten-administratie!

Informatieplicht: transparantie en het recht op informatie
Persoonsgegevens moeten volgens de AVG worden verwerkt op een manier die transparant is voor de betrokkene. Daarmee wordt bedoeld dat degene van wie persoonlijke gegevens worden verzameld, gebruikt, geraadpleegd of anderszins verwerkt duidelijk weet door wie en waarom. Verzamelt u de gegevens niet zelf maar krijgt u ze van derden? Dan bent u verplicht alsnog aan de betrokkene te melden welke gegevens u heeft ontvangen, van wie en met welk doel.
Uw privacystatement moet alle informatie bevatten die voor deze transparantie vereist is. Zorg daarbij dat de privacy-informatie wordt verstrekt vóórdat u gegevens gaat verzamelen. Zet hem op uw site, als pop-up in uw app of als bijlage bij documentatie die u verstuurt. Het verdient aanbeveling uw privacystatement te laten opstellen door een gespecialiseerd bureau of een jurist.

Andere rechten van betrokkenen
Behalve het recht op informatie hebben betrokkenen volgens de AVG ook de volgende rechten:
- recht van inzage
- recht op correctie en verwijdering
- recht op dataportabiliteit.

Leg binnen uw organisatie vast welke informatie waar te vinden is en bereid een correcte en volledige standaardreactie op verzoeken tot inzage, correctie, verwijdering of overdracht voor.

Meldplicht datalekken
Datalekken, de media staan er vandaag de dag bol van. Bewuste ‘strategische’ lekken, vaak met politieke motieven. Abusievelijke lekken door onzorgvuldig omgaan met informatie. Of datalekken als gevolg van internetcriminaliteit. Naast passende maatregelen nemen ter voorkoming van datalekken bent u als ondernemer in de nieuwe privacywetgeving voortaan verplicht om datalekken binnen 72 uur te melden bij de Autoriteit Persoonsgegevens.

Wat is een datalek?
De Wet definieert een datalek als “een inbreuk op de beveiliging, waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijke kans op nadelige gevolgen voor de bescherming van persoonsgegevens die door hem worden verwerkt.”
Datalekkage kan bijvoorbeeld optreden als gegevensdragers of apparaten worden gestolen of verloren, uw server of computer wordt gehackt, uw wachtwoorden te veel voor de hand liggen of er malware terechtkomt op uw computer. Maar ook offline, bijvoorbeeld als u per ongeluk klantgegevens laat liggen bij uw kopieerapparaat.

Wat kunt u doen als ondernemer?
Zorg voor adequate beveiliging, zowel technisch als organisatorisch. Breng in kaart waar zich binnen uw organisatie potentieel datalekken kunnen voordoen. Maak goede afspraken met organisaties die uw data verwerken. En richt procedures in om snel een (potentieel) datalek te onderzoeken en te melden. Zorg ook dat u snel en adequaat kunt reageren als er toch een datalek ontstaat (incident response).

3.4. Organisatorische maatregelen

Van GDPR-/AVG-toetsing tot beveiligingsbeleid, hoe pakken we dat aan?

1. Inventarisatie
2. Overzicht NU: waar staat de organisatie nu op juridisch, technisch en organisatorisch gebied? We lichten het hele netwerk en de hele organisatie door.
3. Inventariseren risico's
4. Advies over STRAKS: wat moet de organisatie doen?
5. Implementatie
6. Evaluatie

Privacy Impact Assessment (PIA)
Als onderdeel van de AVG implementatie voert ID Control bij organisaties vaak een Privacy Impact Assessment (PIA) uit met als hoofdvraag: wat is de impact voor uw organisatie als die persoonsgegevens zou lekken? Deze PIA geeft aanknopingspunten voor het inrichten van privacy-securityprocedures. Bijvoorbeeld bij een Bring-Your-Own-Device policy: wat is uw beleid als iemand op het bedrijfsnetwerk een game downloadt die spyware blijkt te bevatten?

Aandachtspunt: bewustzijn kweken voor privacy
Bij grote organisaties is er veel aandacht voor privacy, veel organisaties stellen een privacy officer aan. Maar de richtlijnen zijn ook toepasbaar voor het MKB. Daar zien we vaak dat er minder aandacht is voor hoe om te gaan met privacy. Deuren van kantoren staan open, USB-sticks slingeren rond. Er vindt veel informatieuitwisseling plaats tussen bedrijfsmails en privémails, soms gaat zelfs alles via privémails. De DGA is klein begonnen en groot geworden, de organisatie is gegroeid en gebruikt allerlei systemen en hulpmiddelen. Maar eigenlijk weet men niet hoe IT werkt.

Privacy is met name een gedragsaspect, een bewustzijn dat moet worden gekweekt bij ieder individu binnen de organisatie. Als de relevante mensen in uw organisatie op de hoogte zijn van de nieuwe privacyregels, kunnen zij inschatten wat de impact is op uw huidige processen, diensten en goederen en welke aanpassingen nodig zijn om aan de AVG te voldoen.

Hoe maken wij uw medewerkers bewust van privacykwesties en hoe om te gaan met gevoelige informatie?
Uw afdeling Human Resources speelt een cruciale rol in het proces. Wij betrekken hen direct bij zaken als beveiligingsbeleid, privacybeleid, verwerkingsregister, procedure melding datalekken en privacy impact assessments.

De nieuwe Europese Privacywetgeving: kostenpost of concurrentievoordeel?

Voor onze opdrachtgevers verzorgen wij awareness-trainingen. Deze trainingen baseren we op wat voor meldingen er binnenkomen bij de Autoriteit Persoonsgegevens. Verder proberen we bewustzijn te kweken onder medewerkers via e-learning. In enkele gevallen hebben we zelfs een interne phishingcampagne opgezet om een shock-effect te bereiken en medewerkers zo met hun neus op de harde feiten te drukken.

Privacy-security beveiligingsbeleid

Als u uw beveiligingsbeleid niet goed op orde hebt, riskeert u een hoge boete. Stel dat u alleen afhankelijk bent van een webshop, zoals Bol.com. Of dat u een klein bedrijf hebt met een goedlopende webshop. Hoe gaat u daarmee om? Of in geval van een medische webapplicatie met heel veel jongeren als patiënt? Stuk voor stuk situaties die vragen om een accuraat privacy-securitybeleid.

Beleid met technische en organisatorische maatregelen voor het omgaan met gevoelige informatie wordt normaalgesproken opgesteld volgens het **BEIC-principe**. BEIC staat voor beschikbaarheid, exclusiviteit, integriteit en controleerbaarheid.

Beschikbaarheid

Een bepalende factor voor beschikbaarheid is hoe u omgaat met back-ups. Stel dat u data van een klant opslaat in de cloud, bijvoorbeeld foto's. En u hebt geen back-up gemaakt. Dan blijkt dat Apple uw data kwijt is. Wat mag u in zo'n geval verwachten van Apple?

Nog een voorbeeld: een gemeente had wel een back-upbeleid maar geen herstelbeleid. Na een calamiteit ontdekte men dat de gemaakte back-ups niet konden worden teruggezet. Met een aanzienlijk dataverlies als gevolg.

Door zelf een goede procedure voor het omgaan met back-ups in te stellen voorkomt u problemen zoals deze. Controleer niet alleen of er daadwerkelijk frequent back-ups worden gemaakt, maar ook of u de back-ups correct kunt herstellen indien nodig. En hoelang back-ups beschikbaar blijven.

Exclusiviteit

De exclusiviteit van uw gegevens staat of valt met een goede toegangsbeveiliging en goede authenticatieprocedures: wie heeft toegang tot welke gegevens en via welke kanalen? Uw VPN bijvoorbeeld, is dat exclusief toegankelijk voor bepaalde gebruikers? In dat geval moet u de identiteit van inloggers controleren aan de hand van een soort sleuteltje.

Integriteit

Goede procedures beschermen de integriteit van uw systemen en processen. Bijvoorbeeld als u facturen automatisch overmaakt op basis van stamdata in het systeem. Wordt uw systeem gehackt en het rekeningnummer vervangen door een rekeningnummer van een katvanger? Dan kan het zomaar gebeuren dat u dit niet in de gaten heeft.

Of een medewerker krijgt een e-mail van de directeur waarin staat dat een factuur nog betaald moet worden. Hoe weet uw medewerker dat dit e-mailbericht inderdaad afkomstig is van die persoon? En hoe weet u dat degene aan wie u e-mailberichten verstuurt ook degene is die ze leest, en dat uw bericht onderweg niet veranderd wordt?

Controleerbaarheid
Goede afspraken vormen de basis van controleerbaarheid. Bijvoorbeeld: tijdens werktijd geen games downloaden of spelen, voetbalwedstrijden kijken, etc. Leg ook de aansprakelijkheid vast: downloadt iemand automatisch iets op het netwerk van het bedrijf, dan kunnen daarop disciplinaire maatregelen staan. In het uiterste geval zelfs ontslag.

3.5. Technische maatregelen

De technische maatregelen om te voldoen aan de AVG hebben betrekking op software, hardware en fysieke beveiliging. Van relatief eenvoudige maatregelen als uw laptop schoonhouden (fysiek en online) tot complexere maatregelen als restricties instellen voor uw VPN zodat alleen bepaalde apparaten verbinding kunnen maken.

Bij fysieke beveiliging kunt u bijvoorbeeld denken aan het verminderen van het risico op diefstal of ontvreemding door de deur van uw serverhok goed af te sluiten, te zorgen dat er altijd iemand bij de receptie is, ramen en deuren goed dicht te doen, etc.

Tot de technische softwaremaatregelen hoort ook het aspect ‘privacy by design’, oftewel bij voorbaat al nadenken hoe de privacy gewaarborgd wordt. Er zijn voorbeelden zat van organisaties die hier niet goed mee omgaan. Windows 10 stuurt bijvoorbeeld al uw zoekopdrachten naar Microsoft. Dat staat ongetwijfeld ergens in de kleine lettertjes en er is natuurlijk ook wel een manier om dit uit te zetten.
Maar in de nieuwe AVG moet de uitgangssituatie zijn dat gegevens pas verzameld, doorgestuurd en/of verwerkt mogen worden na uitdrukkelijke toestemming van de betrokkene.

De AVG schrijft bovendien voor ‘passende’ beveiligingsmaatregelen te nemen om een datalek te voorkomen. De vraag is hierbij: wat zijn ‘passende maatregelen’? Dat blijft voor elke onderneming maatwerk. Maar als u de onderstaande vier gebieden op orde heeft, heeft u het grootste deel te pakken. Omdat de hele keten zo sterk is als de zwakste schakel, verdienen alle categorieën aandacht.

Gebruikersbeveiliging
De gebruiker is de zwakste schakel in cybersecurity. Bij zo’n 45% van de datalekken die nu gemeld worden heeft een werknemer een e-mail met privacygevoelige informatie naar de verkeerde persoon gestuurd. Deels kunt u dit proberen te ondervangen met technische ingrepen, zoals ‘mobile device management’ (beheer, beveiliging en toezicht op mobiele apparaten als smartphones en tablets), datalekpreventie en ‘endpoint protection’.

Maar misschien nog wel belangrijker is bewustwording onder werknemers. De bewustwording neemt toe wanneer er regelmatig aandacht is voor het onderwerp, waarbij heel specifiek voorbeeldgedrag positief wordt belicht. Elke werknemer moet dus weten: wat is een datalek? Hoe kan ik het voorkomen? En wat moet ik doen wanneer ik denk dat er sprake is van een datalek?

Netwerk- en toegangsbeveiliging
Dit zijn de maatregelen die u kunt nemen om te zorgen dat uw bedrijfsnetwerk en de internettoegang veilig zijn en ook blijven functioneren. Dus: een beschermingswal aanleggen tegen hackers, malware en phishing. In ICT-land worden dit soort maatregelen vaak gebundeld in oplossingen die 'unified threat management (UTM)' worden genoemd. In zo'n pakket zitten vaak onder meer een firewall, een virtual private network (VPN), sterke authenticatie, programma's voor 'intrusion prevention', webfilters (beperking van welke internetsites een gebruiker kan openen) en antivirus-software. Om in de gaten te houden of de beveiliging goed zijn werk doet kunt u gebruikmaken van een zogenoemd security operations center. Zo'n systeem signaleert mogelijke dreigingen voor uw bedrijfsprocessen en gegevens, en zet als dat nodig is de tegenaanval in.

Applicatiebeveiliging
Ook uw organisatie gebruikt waarschijnlijk een aantal computerprogramma's die essentieel zijn voor uw bedrijfsvoering. Tegenwoordig zijn deze applicaties steeds vaker te benaderen via een bedrijfsnetwerk (ook door werknemers die thuiswerken). Daardoor zijn ze kwetsbaar.

Mogelijke maatregelen zijn onder meer: een firewall in de applicatie, een 'wasstraat' tegen DDoS-aanvallen, sterke authenticatie, versleuteling van gegevens (encryptie/decryptie), maar bijvoorbeeld ook een penetratietest. En ook hier weer: bewustzijnstrainingen voor uw werknemers.

Gegevensbeveiliging
Ook offline moet u uw zaakjes op orde hebben. Zoals maatregelen om uw serverruimte te beveiligen (een blusinstallatie, toegangscontrole). Verder moet u voorkomen dat draagbare gegevensdragers als USB-sticks onbeheerd rondslingeren. Maar ook het delen, mailen en opslaan van data vindt vaak onveilig plaats.

Mogelijke maatregelen zijn bijvoorbeeld: encryptie, mobile device management, veilig datadelen, aangetekend en verzegeld e-mailen, back-ups maken en meer bewustzijn creëren binnen uw organisatie.

De nieuwe Europese Privacywetgeving: kostenpost of concurrentievoordeel?

4. Van kostenpost naar concurrentievoordeel

Beschouwt u de nieuwe privacywetgeving als meer dan ‘verplicht nummer’ of een kostenpost, dan kan een correcte implementatie van de privacymaatregelen u ook voordeel opleveren. In dit hoofdstuk leest u welke kansen de invoering van de AVG u biedt.

4.1. Accountability en compliance

20-30 jaar geleden was het gebruikelijk dat documentatie werd afgedrukt, opgeslagen in ordners en bewaard in documentatiekamers of kluizen. Wilde u data versturen, dan moest dit correct verpakt gebeuren via het postkantoor, voorzien van een postzegel of bij belangrijke stukken aangetekend. Deze kosten zijn weggevallen door de ontwikkelingen op het gebied van digitalisatie. De Europese wetgever heeft uiteindelijk een level playing field gecreerd waarbij tussen EU-landen niet meer geconcurreerd kan worden op bescherming van persoonsgegevens. Organisaties moeten nu echter wel kosten maken om dat minimale beschermingsniveau te halen.

Hoe belangrijk is compliance voor u en uw organisatie? Kunt u riskeren dat u slecht in het nieuws komt? Wat gaat u uw accountant antwoorden op de vraag of u zich houdt aan alle wet- en regelgeving?

4.2. MVO: grijp de AVG aan als kans

In plaats van de AVG te zien als een verplicht nummer, kunt u als organisatie er ook voor kiezen het nemen van voldoende privacymaatregelen te zien als een MVO-maatregel en in te zetten als unique selling point (USP). U kunt bijvoorbeeld actief inspelen in op de implementatie van de AVG door duidelijk te maken wat u doet voor de bescherming van de persoonsgegevens van uw klanten en medewerkers.

4.3. Reputatiemanagement: geef uw doelgroepen vertrouwen

Als uw server steeds plat gaat, gaat het op den duur in uw nadeel werken. En u loopt reputatieschade op. Zeker als u door securityproblemen of privacy-issues uw core business niet kunt leveren. Bijvoorbeeld internetbankieren; als dat het niet meer doet, wat dan? In Estland gingen enige tijd geleden alle pinautomaten plat door een Russische aanval.

Niet data maar vertrouwen is het nieuwe goud. Privacy niet op orde? Dan gaan uw klanten gewoon naar een concurrent. Laat dit in uw voordeel werken door – minimaal in uw privacystatement - duidelijk en open te communiceren welke persoonsgegevens u verzamelt en verwerkt, voor welke doeleinden, via welke verwerkers en hoe uw doelgroepen hun rechten kunnen uitoefenen. Laat zien dat u het privacyvraagstuk zeer serieus neemt en hoe u de privacy van uw klanten en businesspartners waarborgt. Kortom: geef ze het vertrouwen dat de privacy van hun persoonsgegevens bij u goed geregeld is.

5. Over de auteurs

Kees Gordijn, partner bij CFO Capabel

Veranderend klantgedrag en ICT hebben enorme impact op een onderneming: keuzes maken, de beweging inzetten en de medewerkers meekrijgen. Waar begin je en hoe doe je dat? Hoe maak je de vertaling van strategie naar operatie? Kees gelooft in 'Viral Change'; je moet bewogen raken om in beweging te komen. Als partner bij CFO Capabel helpt hij organisaties bij het maken van strategische keuzes en het professionaliseren van het (financieel) management. Hij stond aan de basis van grote veranderingen en vernieuwingen op het gebied van financial en process control, HR, (krediet)risicomanagement, fusies, distributie en huisvesting.

Hans Kortekaas, Directeur bij ID Control

12 jaar geleden als oprichter van ID Control aan de slag gegaan met een idee hoe organisaties en individuen het digitale goud (de data kroonjuwelen) het beste kunnen beschermen. Informatie is macht en hij vindt dat de controle hierover bij de organisatie of het individu hoort te liggen en niet bij derden. Hans werkt als directeur binnen ID Control op het gebied van innovatieve Europese privacy en cyber security producten en diensten en is met name bezig de propositie naar organisaties en individuen continue te verbeteren.

Rembrandt de Haan, Privacy Consultant bij ID Control

Al jaren bevlogen in privacy. Heeft hij wat te verbergen? Ja natuurlijk! Maar Rembrandt vindt dat daarmee niets mis is. Hij gaat uit van het positieve van de mens. Rembrandt heeft een achtergrond als jurist en heeft lang geadviseerd over compliancy, privacy, juridische en organisatievraagstukken. Laatstelijk binnen de Zorgsector met al haar privacyzorgen. Hij ervaart het werk bij het Europese Privacy Bedrijf ID Control als een missie. Rembrandt werkt binnen ID Control als Privacy Consultant op het snijvlak van juridisch, technisch en organisatorisch advies.

De nieuwe Europese Privacywetgeving: kostenpost of concurrentievoordeel?

ID Control is de Europese Privacy- en Cybersecurity-specialist die zorgt voor passende technische, organisatorische en juridische beveiligingsmaatregelen om organisaties te beschermen tegen digitale risico's en dreigingen.

ID Control
Van Diemenstraat 202
2518 VH Den Haag

T : +31 888 SECURE (732873)
E : info@idcontrol.com
W : www.idcontrol.com

CFO Capabel helpt organisaties in het MKB op praktische en concrete wijze bij het maken van de juiste (strategische) keuzes en het professionaliseren van het financieel management. Dit doen we door de inzet van gedreven en ervaren financieel directeuren, zowel op interim-basis – onze parttime CFO's - als op basis van werving & selectie voor uw vaste vacatures.

CFO Capabel
De Helling 6
3911 VA Rhenen

T: +31 (0)653241259
E: kees.gordijn@cfocapabel.nl
W: www.cfocapabel.nl

De nieuwe Europese Privacywetgeving: kostenpost of concurrentievoordeel?

6. Bronnen

- *Autoriteit Persoonsgegevens*: ttps://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/europese-privacywetgeving/algemene-verordening-gegevensbescherming
- *Europese Commissie*: http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_nl.htm#mobile-menu
- *Cybersecurity and SOX*: https://www.a2q2.com/blog/sox/29-cyber-security-and-sox/
- *Nederland ICT*: https://www.nederlandict.nl/news/de-avg-uitgelegd-deel-2-transparantie-en-het-recht-op-informatie/
- Diverse nieuwsartikelen op *Nu.nl*