Ga jij al discreet om met persoonsgegevens?

Whitepaper

LanTel®
Improving business communication

N LanTel B.V.
A Pieter Zeemanweg 57
W 3316 GZ Dordrecht

T 078 – 630 55 55
E info@lantel.nl
I www.lantel.nl

Inhoudsopgave

1. Wat is de AVG?

De “Algemene Verordering Gegevensbescherming (AVG)”, in het Engels “General Data Regulation (GDPR)”, is een Europees gereguleerde privacy verordening. De verordening gaat over het beschermen van de persoonsgegevens van natuurlijke personen en het vrije verkeer van die gegevens. AVG is de vervanger van de Databeschermingsrichtlijn die inmiddels uit 1995 stamt. Gebleken is dat deze niet meer aansluit bij het huidige digitale tijdperk.
Europese regulering is bovendien een groot voordeel omdat de Europese lidstaten op dit moment nog hun eigen nationale wetten hanteren. Per 25 mei 2018 is dit centraal geregeld middels de AVG. Doordat veel regels uit de Wet bescherming persoonsgegevens (Wbp) zijn overgenomen in de AVG, komt de Wbp te vervallen.

1.1 Waarom een wijziging?

In de EU hebben alle lidstaten een eigen privacywet. Alhoewel alle nationale wetten van de EU-lidstaten wel zijn gebaseerd op de Europese privacyrichtlijn uit 1995, is de tijd er nu rijp voor om dit centraal te reguleren. Daarnaast stammen de huidige wetten uit 1995; een periode waarin het internet nog in de kinderschoenen stond. Ga maar na: mobiel internet bestond nog niet, het thuisinternet kwam pas net op en de pc zoals wij die nu kennen werd pas echt een hebbeding door de introductie van Windows 95. En herinner je deze telefoons nog?

De hoogste tijd dus voor een update, want de wetgeving omtrent digitale middelen is te summier en dekt zeker niet meer de lading van de moderne tijd. De combinatie van deze twee factoren heeft geleid tot de invoering van de AVG.

1.2 Principes

Er zijn een aantal principes die ten grondslag liggen aan de AVG, allen met het doel de persoonsgegevens van natuurlijke personen beter te beschermen. Dit zijn:

Transparantie
De persoon van wie de gegevens verwerkt worden, is van deze verwerking op de hoogte, heeft hier toestemming voor gegeven en is zich bewust van zijn rechten (waaronder het recht op vergetelheid en het recht op dataportabiliteit – zie ook 1.4).

Doelbeperking
De persoonsgegevens mogen alleen gebruikt worden voor het doel waarvoor de gegevens in eerste instantie zijn verzameld. Als je een mailinglijst hebt aangelegd voor een nieuwsbrief, mag je deze gegevens dus niet gebruiken om een directe salesaanbieding te doen.

Gegevensbeperking
Enkel de noodzakelijke gegevens die voor het beoogde doel benodigd zijn, mogen worden verzameld. Een intranet is bijvoorbeeld een plek waar veel gegevens gevraagd worden – naam, e-mailadres, telefoonnummer, sociale profielen. Alles wat niet nodig is om gebruik te kunnen maken van het intranet, mag dan niet verzameld worden.

Juistheid
De persoonsgegevens moeten correct zijn en blijven.

Bewaarbeperking
De persoonsgegevens mogen niet langer bewaard worden dan nodig voor het beoogde doel.

Integriteit en vertrouwelijkheid
De persoonsgegevens moeten beschermd worden tegen toegang door onbevoegden, verlies of vernietiging.

Verantwoording
De verantwoordelijke moet kunnen aantonen aan deze regels te voldoen.

Door deze principes in acht te nemen wordt de privacy van de eindgebruiker beter beschermd. Goede zaak zou je zeggen, maar wel een die niet zonder haken en ogen is. Voor ZZP'ers, MKB'ers en ondernemers verandert er nogal wat.

1.3 Wanneer wordt de AVG-verordering van kracht?

De AVG is inmiddels van kracht, maar per 25 mei 2018 mag er ook gehandhaafd gaan worden. Vanaf dat moment moeten alle bedrijven kunnen aantonen dat ze voldoen aan de AVG-regelgeving.

1.4 Wat merkt de eindgebruiker van de AVG-verordering?

Eindgebruikers zullen straks merken dat het makkelijker en duidelijker wordt om hun "toestemming" te geven en/of in te trekken. Hun privacyrechten worden aanzienlijk verbeterd. Er zijn tevens een tweetal aanvullende rechten gedefinieerd die de eindgebruiker nog beter beschermen. Dit zijn:

Recht op vergetelheid

Op dit moment heeft de eindgebruiker al het recht om een organisatie te vragen hun persoonsgegevens te verwijderen. Aanvullend hierop kunnen eindgebruikers eisen dat de organisatie de verwijdering doorgeeft aan alle andere organisaties aan wie zij de gegevens hebben doorgegeven.

Recht op dataportabiliteit

Eindgebruikers kunnen straks vragen aan bedrijven om de opgeslagen gegevens in een standaardformaat te ontvangen. Deze gegevens kunnen zij dan op een makkelijke manier doorgeven aan een andere leverancier van dezelfde soort dienst. Indien technisch haalbaar kunnen zij zelfs vragen of het bedrijf hun persoonsgegevens direct doorstuurt aan de nieuwe dienstverlener.

2. Welke gevolgen heeft de AVG?

De verordening heeft nogal wat gevolgen voor bedrijven die met persoonsgegevens werken. Er verandert veel, en de boetes bij het niet naleven van de verordening zijn niet mals. Een goede voorbereiding is dus van belang zodat de deadline ook daadwerkelijk gehaald wordt.

2.1 Wat zijn de belangrijkste wijzigingen van de AVG voor organisaties?

Door de invoering van de AVG hebben bedrijven meer verplichtingen bij het verwerken van persoonsgegevens. Daarnaast wordt de verantwoordelijkheid om aan te tonen dat men de wet naleeft nog meer bij de bedrijven zelf gelegd. Bedrijven moeten op ieder ogenblik kunnen aantonen dat zij zich aan de wettelijke bepalingen houden. Ook moeten bedrijven kunnen aantonen dat zij de juiste technische en organisatorische maatregelen hebben genomen om te (blijven) voldoen aan de AVG-verordening. Deze set van maatregelen heet de verantwoordingsplicht.
Deze plicht geldt voor alle bedrijven die met persoonsgegevens werken. Zij moeten verantwoording af kunnen leggen aan de Autoriteit Persoonsgegevens, de organisatie die in Nederland verantwoordelijk is voor de controle op het naleven van de regels voortvloeiend uit de AVG door organisaties.

Boetes

Een andere belangrijke wijziging zit in het boetebedrag bij het niet naleven van de verordening. Bij overtreding van de huidige privacywet is de maximale boete 900.000 euro; het maximale boetebedrag onder AVG bedraagt 20.000.000 euro (20 miljoen) of, indien dit bedrag hoger ligt, 4% van de wereldwijde jaaromzet. Voor grote multinationals kunnen de boetes dus flink oplopen. Ter illustratie: Philips boekte over 2016 een omzet van 24,5 miljard euro, wat de maximale boete op 980 miljoen euro stelt. Maar liefst bijna 1100 keer de huidige maximale boete.

Europees Comité voor Gegevensbescherming

Per Europese lidstaat moet er een autoriteit worden aangewezen die toeziet op de juiste naleving van de AVG, en waar nodig sancties uitdeelt. In Nederland is dit de Autoriteit Persoonsgegevens. Nieuw is de oprichting van een Europees comité welke toeziet op de juiste toepassing van de AVG-regelgeving binnen lidstaten. Dit Europese Comité voor Gegevensbescherming wordt een orgaan van de EU, krijgt rechtspersoonlijkheid en treedt volledig onafhankelijk op.

Functionaris voor Gegevensbescherming

Het kan voorkomen dat je als bedrijf een Functionaris voor Gegevensbescherming (FG) aan moet stellen. Er zijn drie soorten organisaties die verplicht zijn een FG aan te stellen:

1. Overheidsinstanties
2. Organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen. Denk aan cameratoezicht en het monitoren van de gezondheid via wearables.
3. Organisaties die vanuit hun kernactiviteiten op grote schaal bijzondere persoonsgegevens verwerken. Denk aan ziekenhuizen en patiëntendossiers.

Wat "op grote schaal" precies inhoudt specificeert de AVG niet. De criteria die gehanteerd worden zijn het aantal betrokken mensen van wie de gegevens verwerkt worden, de hoeveelheid gegevens, de duur van de gegevensverwerking en de geografische reikwijdte van de verwerking.

De taken van een FG zijn o.a. het creëren van privacy-bewustzijn in de organisatie, het monitoren van de wijze waarop de organisatie met persoonsgegevens omgaat, het toezien op naleving van de privacywetgeving en het functioneren als aanspreekpunt voor de Autoriteit Persoonsgegevens. Meer informatie over de FG is te vinden in de "Richtlijnen voor functionarissen voor gegevensbescherming" van de Autoriteit Persoonsgegevens.

Transparantie

Op dit moment schrijven de privacyrichtlijnen voor dat persoonsgegevens "in overeenstemming met de wet" moeten zijn. Ook moeten persoonsgegevens "behoorlijk en zorgvuldig" verwerkt worden. De AVG doet hier nog een schepje bovenop. In de AVG staat dat de verwerking van gegevens ook "transparant voor de betrokkenen" moet zijn.
Onder transparantie wordt verstaan dat het voor de betrokkene duidelijk is dat zijn gegevens worden verzameld, gebruikt of op een andere manier verwerkt worden, waarom dit gebeurd en door wie dit gebeurd. Dit houdt dus in dat duidelijke communicatie nog belangrijker is. Je moet antwoorden geven op vragen als wie ben je, wat doe je met de verzamelde gegevens, waarom verzamel je die eigenlijk, wat doe je verder nog met die gegevens, hoe kan de betrokkene de gegevens wijzigen en ga zo maar door. Dit moet bovendien binnen een maand na aanmelding gecommuniceerd worden. Ook gegevens die je niet zelf rechtstreeks hebt verwerkt vallen onder deze verplichting. Openheid is dus een absolute must.

Privacy by Design & Privacy by Default

De termen Privacy by Design en Privacy by Default zijn niet nieuw. Wel nieuw is dat deze twee expliciet worden benoemd in artikel 25 van de AVG als zijnde "verplicht door verwerkingsverantwoordelijken om invulling aan te geven". Het is binnen de AVG dus van groot belang om deze plichten op orde te hebben.

Privacy by design betekent dat je in een zo vroeg mogelijk stadium technische en organisatorische maatregelen neemt om zorgvuldig met persoonsgegevens om te kunnen gaan. Bij de ontwikkeling van je product of dienst moet er daarom al aandacht zijn voor de privacy van de eindgebruiker. Stel jezelf de vraag of de gegevens écht nodig zijn of dat je ook met geanonimiseerde gegevens kunt werken. En als je dan toch met persoonsgegevens werkt, denk dan goed na over de beveiliging van deze gegevens. Tot slot moet je oog hebben voor data-minimalisatie, oftewel: waarborg in je ontwerp dat er niet meer persoonsgegevens worden opgeslagen dan strikt noodzakelijk.

Privacy by default is onderdeel van privacy by design, en wil zoveel zeggen als dat persoonsgegevens nooit zomaar openbaar zichtbaar mogen zijn, tenzij de eindgebruiker hier expliciet toestemming voor geeft. Denk aan een social media profiel dat openbaar zichtbaar gemaakt kán worden. Standaard hoort dit dus niet openbaar te zijn!

Om op een begrijpelijke manier de begrippen in je organisatie uit te leggen heeft Privacy Company dit framework ontwikkeld. Het biedt praktische handvatten om meer inzicht te bewerkstelligen binnen de organisatie.

Recht op inzage en recht op rectificatie

Het recht op inzage en recht op rectificatie houdt zoveel in dat een betrokkene inzicht moet kunnen krijgen in de gegevens die er van hem/haar verwerkt worden, en deze waar nodig moet kunnen rectificeren. Er kan een inzageverzoek worden gedaan, waarbij tenminste de volgende informatie moet worden verstrekt:

1. De verwerkingsdoeleinden.
2. De categorieën van gegevens.
3. De ontvangers aan wie de gegevens verstrekt worden, vooral als dit ontvangers in landen buiten de Europese Economische Ruimte zijn.
4. Bij doorgifte naar een ander land: wat de passende waarborgen in dat land zijn.
5. De duur van de opslag van de gegevens.
6. Het feit dat de betrokkene recht heeft op rectificatie, beperking van de verwerking en bezwaar.
7. Dat de betrokkene bezwaar kan maken bij de toezichthouder.
8. Wat de bron van de gegevens is.
9. Indien er sprake is van geautomatiseerde besluitvorming of profiling: wat de daaraan ten grondslag liggende logica is en de gevolgen van de verwerking zijn.
10. Een kopie van de persoonsgegevens zelf.

Mocht blijken dat de gegevens niet correct zijn dan heeft de betrokkene recht op het rectificeren van deze gegevens. Dit kan een verwijdering van onjuiste gegevens zijn, maar ook een aanvulling op bestaande gegevens middels een aantekening.

Recht op vergetelheid

Het recht op vergetelheid betekent dat de eindgebruiker het recht heeft om “vergeten” te worden, oftewel: het verwijderen van zijn/haar gegevens uit de database indien er geen goede reden meer is om de gegevens nog langer te bewaren. Het moet voor eindgebruikers daarnaast ook duidelijk zijn waar ze met hun verzoek tot vergetelheid terecht kunnen in de organisatie. Het recht op vergetelheid is niet absoluut. Er kan een beroep op worden gedaan in de volgende gevallen:

1. De persoonsgegevens zijn niet langer meer nodig voor de doeleinden waarvoor ze zijn verzameld of anderszins verwerkt.
2. De betrokkene trekt zijn eerder gegeven toestemming in. De betrokkene moet zijn toestemming op dezelfde manier kunnen intrekken als dat hij hem gegeven heeft.
3. De betrokkene maakt bezwaar tegen de verwerking voor zijn specifieke situatie en er zijn geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking.
4. De betrokkene maakt bezwaar tegen de verwerking van zijn gegevens t.b.v. direct marketing inclusief daaraan gerelateerde profiling.
5. De persoonsgegevens zijn onrechtmatig verwerkt.
6. De gegevens moeten gewist worden om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.
7. Het gaat om toestemming gegeven door/voor minderjarigen voor diensten van de informatiemaatschappij (zoals social networks of online games).

De meeste van deze redenen liggen erg voor de hand, maar oplettendheid is geboden bij punt 3. Stel je voor dat een geesteszieke patiënt aan een arts vraagt de gegevens over zijn/haar aandoening uit het medisch dossier te verwijderen. De arts is dan niet verplicht de gegevens te verwijderen omdat er een prevalerende, gerechtvaardigde grond voor de verwerking is. Andersom kan iemand die bijvoorbeeld een celstraf heeft uitgezeten wel een beroep doen op het recht op vergetelheid, omdat diegene zijn/haar straf heeft uitgezeten en diegene niet steeds geconfronteerd hoeft te worden met deze oude veroordeling.

Recht op dataportabiliteit

Tot slot hebben eindgebruikers het recht op dataportabiliteit gekregen. Dit betekent dat het voor eindgebruikers makkelijker wordt om van dienstverlener te wisselen. Dit kan de eindgebruiker doen door zijn/haar gegevens op te vragen bij de dienstverlener, bijvoorbeeld een zorgverzekeraar. Deze partij moet de gegevens dan op een gestructureerde, gangbare en door computers inleesbare wijze aangeleverd worden zodat deze aan de nieuwe dienstverlener verstrekt kunnen worden. Het gaat hierbij alleen om de "eigen" data van de persoon en het moet altijd gaan om een geautomatiseerde verwerking. Data van derden wordt er dus uitgehaald. Meer informatie over richtlijnen en concrete voorbeelden zijn te vinden op de site van de Autoriteit Persoonsgegevens – richtlijnen voor het recht op dataportabiliteit.

Privacy Impact Assessment

Vooraf nadenken over de privacy-risico's van je dataverwerking is een must bij de AVG. Het doen van een Privacy Impact Assessment is hierbij het aangewezen – en in sommige gevallen zelfs verplicht gestelde – middel. Dit assessment heeft als doel het verkleinen van de risico's doordat je vooraf deze risico's inventariseert, en nadenkt over logische stappen om dit risico te verkleinen. Het instrument is niet nieuw, echter de verplichting is dat wel. Deze geldt bij verwerkingen die een groot privacy-risico met zich meebrengen. Denk aan grootschalige verwerking van bijzondere persoonsgegevens of het continu monitoren van publiek toegankelijke ruimten. Bepaal eerst of een PIA nodig is, breng daarna de impact op de privacy in kaart en kijk of je maatregelen kunt nemen om deze impact zoveel mogelijk te verkleinen. Lukt dit niet dan ben je verplicht de Autoriteit Persoonsgegevens te raadplegen. Tot slot maak je een rapportage waarin je de PIA uitkomsten opschrijft.

2.2 Welke voordelen biedt deze verordering voor bedrijven?

Het grootste voordeel van de AVG is de eenduidigheid die straks geldt voor de gehele EU. Je hoeft dus geen rekening meer te houden met alle lokale wetten en regels op het gebied van privacy, maar weet zeker dat je "privacy-proof" bent in de hele EU. Voor bedrijven die zaken doen met of in het buitenland een geruststellende gedachte. Daarnaast zorgt de AVG voor een gelijk speelveld omdat straks overal dezelfde richtlijnen gelden. Dit zorgt voor een eerlijke markt met gelijke mogelijkheden voor alle organisaties uit de EU-lidstaten.

Niet geheel onbelangrijk is dat ook de kosten omlaag zullen gaan. Je hoeft immers nog maar met één toezichthouder zaken te doen (one-stop-shop), in plaats van met meerdere lokale toezichthouders. Dit zou de doorlooptijd van procedures in theorie ook moeten verkorten.

Tot slot is er een grote marketingkans voor bedrijven die vol met de AVG aan de slag zullen gaan. De AVG zal als betrouwbaar "keurmerk" gezien worden door eindgebruikers. Bedrijven die vanuit hun diepste overtuiging zorgvuldig met persoonsgegevens omgaan, en dit ook uitstralen, zullen

sneller vertrouwd worden dan andere bedrijven. Eindgebruikers zijn dan sneller geneigd hun gegevens aan je toe te vertrouwen. Zo beïnvloedt de verordening de klantperceptie positief; doe er je voordeel mee.

2.3 Is deze verordering ook op mijn organisatie van toepassing?

Als je persoonsgegevens verwerkt is het antwoord hoogstwaarschijnlijk "Ja". En dit doe je al heel snel. Ben je ZZP'er of MKB'er, en bezig met het verwerken van persoonsgegevens? Ook dan geldt de AVG! Zelfs al gaat het om het bijhouden van afspraken met klanten, hun telefoonnummers of personeelsinformatie; de AVG is heel breed, en zorgt voor eenduidigheid op al deze vakken. Maar hierdoor raakt het dus ook heel erg veel bedrijven. Ook al raakt het niet direct je eigen organisatie dan is het wel goed om hierover na te denken. Voorbeeld is een ZZP'er die als webdesigner werkt. Je hoeft niet direct zelf iets te ondernemen, maar wanneer je bijvoorbeeld een webshop voor een klant oplevert, is het wel goed om deze klant te wijzen op de AVG-verordening. Ook hier geldt dat men zich positief kan onderscheiden ten opzichte van de concurrentie.

Enige uitzondering op de verordening vormen politie en justitie wanneer zij hun taken uitvoeren voor de opsporing en vervolging van strafbare feiten en het ten uitvoer leggen van straffen. Ook taken ter bescherming van de openbare veiligheid vallen hieronder, omdat dit nodig is voor het bewaken van de algehele openbare veiligheid. Zij hebben daarom speciale bevoegdheden nodig, die zijn vastgelegd in de Richtlijn gegevensbescherming Politie. Alle EU-lidstaten zijn verplicht deze richtlijnen in hun nationale wetgeving te implementeren.

3. Help, ik snap er niets van! Waar begin ik?

Er komt nogal wat nieuwe informatie op je af met de nieuwe verordening. Hoofdstuk 2 van deze whitepaper bevat alle noodzakelijke informatie om AVG-compliant te worden. Om je alvast op weg te helpen om richting compliancy te komen hebben wij een stappenplan bedacht dat de route richting compliancy vergemakkelijkt.

Stap 1. Begin met bewustwording in de organisatie
Schuif de voorbereidingen niet op de lange termijn, maar begin er nu aan. En begin in de organisatie. Heb het met de relevante mensen in de organisatie over de impact van de AVG. Zijn er aanpassingen nodig om te voldoen aan de AVG? Praat er eens over met leveranciers. En, met klanten. Zijn bijvoorbeeld je bewerkersovereenkomsten op orde?

Stap 2. Creëer inzicht
Inventariseer hoe je organisatie nu omgaat met persoonsgegevens. Heb je alle data van je klanten wel nodig? En zo ja, wat doe je er dan mee? Maak eens een schematische weergave van de gegevens, doelverwerkingen en bewaartermijnen om inzicht te creëren. Waar komen gegevens vandaan en met wie delen we deze gegevens? Wanneer de gegevensverwerking een hoog risico op privacyschending met zich meebrengt kan de organisatie verplicht zijn een zogenaamde Privacy Impact Assessment (PIA) uit te voeren. Schat nu alvast in of je een PIA moet uitvoeren. Kortom, creëer inzicht en zorg ervoor dat de juiste mensen binnen de organisatie van de nieuwe privacyregels op de hoogte zijn.

Stap 3. Privacy by design & Privacy by default
Hou nu al bij het ontwerpen van producten en/of diensten rekening met ‘Privacy by design’ en ‘Privacy by default’, ook al is de verordening nog niet van kracht. Neem de nodige technische en organisatorische maatregelen om ervoor te zorgen dat je alleen persoonsgegevens verwerkt voor het specifieke doel dat je wil bereiken.

Stap 4. Maak beleid
Zorg dat je de verplichtingen uit de AVG die gelden voor jouw organisatie vertaald naar helder beleid. Denk daarbij onder andere aan een beveiligingsbeleid, beleid met betrekking tot het omgaan met datalekken, beleid met betrekking tot het omgaan met rechten van de betrokkenen en beleid voor de toepasselijke bewaartermijnen en het gebruik maken van bewerkersovereenkomsten. Vernieuw vervolgens je privacy statements, zowel voor je klanten en websitebezoekers als voor je werknemers.

Stap 5. Heb je een functionaris voor de gegevensbescherming nodig?
Ga na of je een functionaris voor de gegevensbescherming nodig hebt die toezicht houdt op de naleving van de AVG verordening. Stel er één aan indien nodig.

Stap 6. Neem de tijd
Begin NU, schuif het niet voor je uit want anders ben je te laat. Begin met het creëren van inzicht binnen je eigen organisatie alvorens met de overige stappen verder te gaan. Zorg ervoor dat je organisatie goed voorbereid is.

Stap 7. Accepteer AVG als een onderdeel van je bedrijfsvoering

De AVG gaat er hoe dan ook komen. Zorg er daarom voor dat je het accepteert, de verplichtingen in acht neemt en het in je bedrijfsvoering integreert, zodat het een wezenlijk onderdeel van het beslistraject wordt.

4. Waar kan ik terecht met mijn verdere vragen?

Deze whitepaper is slechts een greep uit de volledige teksten. Het geeft je wel goede handvatten en een leidraad om verder te gaan. Om je nog verder op weg te helpen kun je onderstaande bronnen raadplegen.

Autoriteit persoonsgegevens
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/

Nederland ICT
https://www.nederlandict.nl/dossier/avg/

Thuiswinkel waarborg
https://www.thuiswinkel.org/bedrijven/belangenbehartiging/privacy/algemene-verordening-gegevensbescherming/avg

AVG op Rijksoverheid.nl
https://www.rijksoverheid.nl/documenten/rapporten/2016/01/07/tk-bijlage-1-council-of-the-european-union

AVG de volledige teksten
https://www.privacy-regulation.eu/nl