sebyde
secure by design

Privacywetgeving:

AVG /GDPR

Wat betekent dat voor u?

ISD
IT solutions in green

Introductie:

Geachte TSD-Relatie,

Op dinsdag 16 januari jl. hebben wij tijdens een door TSD IT b.v. georganiseerde bijeenkomst een tweetal presentaties gegeven over de AVG (GDPR). De belangrijkste aspecten van de AVG, wat dat voor bedrijven betekent en wat gedaan moet worden om op de AVG in te spelen, kwamen uitgebreid aan bod.

Tijdens de bijeenkomst is aan een ieder toegezegd naast de hand-out van de presentatie enige samenvattende toelichting te versturen.
Een aantal anderen, die helaas verhinderd was, heeft specifiek gevraagd om de toezending van informatie. Voor hen is deze toelichting vast ook praktisch.

Met vriendelijke groet,

Sebyde BV

Rob Koch
rob.koch@sebyde.nl

Inleiding

Er zijn belangrijke ontwikkelingen in de privacywetgeving. Dit heeft consequenties voor het bedrijfsleven.

Ter vervanging van de verschillende privacywetgevingen die binnen de Europese lidstaten worden gebruikt, is er per April 2016 een nieuwe Europese Privacywetgeving ingegaan. Dit is de **AVG** (Algemene Verordening Gegevensbescherming). De Engelse benaming van deze wetgeving is: **GDPR** (General Data Protection Regulation).

De GDPR is van toepassing in alle 28 lidstaten van de Europese gemeenschap.
Deze wetgeving stelt serieuze eisen aan de bescherming en het waarborgen van de privacy van persoonsgegevens. Bedrijven en organisaties hebben daarom 2 jaar de tijd gekregen om zich op de GDPR voor te bereiden. In Mei 2018 zal door de 28 Europese autoriteiten gestart worden met de handhaving van de GDPR. De huidig geldende wetgeving (in Nederland is dat de Wbp, Wet Bescherming Persoonsgegevens) zal dan komen te vervallen.

Belangrijke dingen om te weten over de AVG!

Persoonsgegevens:

Persoonsgegevens zijn gegevens die direct of indirect te herleiden zijn naar individuele personen. Persoonsgegevens worden in feite in twee categorieën verdeeld: "normale" en "bijzondere" persoonsgegevens. Met "normale" persoonsgegevens worden gegevens zoals bijvoorbeeld een emailadres of een telefoonnummer bedoeld. Onder de categorie "bijzonder" vallen gegevens die, bij het uitlekken daarvan, inbreuk kunnen maken op de privacy van mensen waarvan deze mensen hele negatieve gevolgen kunnen ervaren (*inbreuk op rechten en vrijheden*). Gedacht moet dan bijvoorbeeld aan gegevens over ziekteverzuim of een burgerservicenummer. Gegevens die de meeste bedrijven van hun medewerkers in bezit hebben.

Persoonsgegevens die gekoppeld zijn aan bedrijven zijn ook persoonsgegevens binnen de reikwijdte van de AVG. De naam van een contactpersoon en diens functie binnen een bedrijf bijvoorbeeld. Zo is een emailadres zoals k.lant@boomkwekerij.nl. een persoonsgegeven.

Verwerken:

Alles wat u met deze gegevens kunt doen, valt onder de noemer "verwerking van persoonsgegevens". Voorbeelden hiervan zijn: opslaan, inzien, muteren, deleten, verspreiden, printen, kopieren, back-up maken, etc. etc. Om binnen de AVG persoonsgegevens op de juiste manier te verwerken, moet er een gerechtvaardigde grondslag zijn. Een arbeidsovereenkomst met een medewerker is bijvoorbeeld een grondslag om diens persoonsgegevens te mogen verwerken. Een zakelijke overeenkomst vormt ook een grondslag voor het verwerken van persoonsgegevens. Er moet wel relevantie zijn. Een gepersonaliseerd emailadres, zoals k.lant@boomkwekerij.nl en de functie van deze persoon heeft relevantie binnen een zakelijke verbinding maar het bewaren van informatie over diens lidmaatschap van een sportclub zeer waarschijnlijk niet. Kortom, om gegevens te mogen verwerken moet er een grondslag zijn. Ook moeten gegevens relevant zijn voor het doel waar die gegevens voor dienen en mogen ze alleen voor dát doel gebruikt worden.

Gebruiken en delen van persoonsgegevens:

Elk bedrijf verwerkt gegevens die te herleiden zijn naar personen. Denk maar eens aan het klanten- of relatie-bestand en het eigen personeelsbestand. Ook worden er door bedrijven vaak persoonsgegevens verwerkt die van andere organisaties afkomstig zijn. In al deze gevallen moet je voldoen aan de privacywetgeving.

Ieder bedrijf is en blijft verantwoordelijk voor de persoonsgegevens die zijn toevertrouwd. Binnen de AVG wordt dit de "verwerkersverantwoordelijke" genoemd. Ook wanneer er andere partijen (verwerkers) betrokken zijn bij verwerkingen, blijft die verwerkersverantwoordelijke aansprakelijk. Bijvoorbeeld werk dat u laat uitvoeren (uitbesteden van een taak) door een arbodienst, salarisverwerker of clouddienst. Het is daarom erg belangrijk om er zeker van te zijn dat die ingeschakelde derde partijen (verwerkers) heel zorgvuldig met uw persoonsgegevens omgaan en dit vast te leggen.

Verwerkersovereenkomsten:

Indien u gebruik maakt van verwerkers dient met een dergelijke partij een verwerkersovereenkomsten afgesloten te zijn. Verwerkersovereenkomsten bevatten informatie over hoe beide partijen omgaan met de wetgeving, welke verwerkingen er worden gedaan op uw gegevens, de aansprakelijkheid in geval van boetes en het niveau van de securitymaatregelen die de verwerker heeft getroffen om uw persoonsgegevens te beschermen.

Marketing:

Voor marketing- en/of reclameachtige uitingen aan personen moet er sprake zijn van toestemming. We kenden allemaal al de verplichting dat iemand "zich moet kunnen uitschrijven voor een nieuwsbrief" maar nu moet vooraf toestemming zijn gegeven, de zogenoemde "OPT-IN". Belangrijk om te weten is dat deze gegevens vastgelegd moeten kunnen worden. Geregistreerd moet worden welke "opt-in" iemand heeft gegeven en of iemand misschien een "opt-out" heeft ingediend.

Recht op inzage, correctie en vergeten worden:

Op grond van de AVG heeft een natuurlijk persoon het recht om in te zien welke gegevens van hem of haar bij een organisatie in bezit zijn. Als hiertoe een verzoek wordt ontvangen dan moet deze worden uitgevoerd. Iemand kan vervolgens verzoeken om gegevens te corrigeren als deze niet correct blijken. Daarnaast kan iemand een verzoek indienen om de gegevens over te dragen aan een andere partij en kan ook verzoeken om de gegevens te verwijderen (een beroep op "het recht om vergeten te worden"). Dit soort verzoeken moeten binnen een bepaalde termijn worden uitgevoerd tenzij er een dwingendrechtelijke grondslag is om de gegevens niet te verwijderen.

Bijvoorbeeld: Als een geïnteresseerde die regelmatig nieuwsbrieven ontvangt niet meer zo geïnteresseerd is en verzoekt om de gegevens te verwijderen dan zal dat moeten worden uitgevoerd. Wanneer een ex-medewerker terstond na vertrek verzoekt om volledige verwijdering van diens gegevens dan kan dat niet omdat er wettelijke verplichtingen zijn om die gegevens een bepaalde periode te bewaren.

Informeren:

Duidelijkheid en transparantie over hoe een organisatie omgaat met de persoonsgegevens die zijn toevertrouwd, is relevant. Het is daarom verplicht om een privacyverklaring te hebben. Voordat iemand besluit "in zee" te gaan met een organisatie moet die persoon informatie beschikbaar hebben waaruit blijkt hoe met persoonsgegevens wordt omgegaan. Zo'n privacyverklaring zal in ieder geval op de website inzichtelijk moeten zijn.

Functionaris Gegevensbescherming:

Binnen de AVG is het voor een aantal organisaties verplicht om een FG (Functionaris Gegevensbescherming) aan te stellen. Een FG houdt toezicht op het naleven van de regelgeving rondom de verwerking van persoonsgegevens. Dit kan een interne medewerker zijn maar ook een externe partij. Voor de meeste MKB-bedrijven die geen *bijzondere* persoonsgegevens verwerken, zal de FG-functie niet verplicht zijn. Wel is het verstandig om te regelen dat als er een situatie ontstaat waarbij die specifieke kennis en kunde nodig is, er een partij is om advies in te kunnen winnen (bijvoorbeeld bij een Datalek). Op de website van de Autoriteit Persoonsgegevens is terug te vinden in welke situaties een FG verplicht is.

AVG (GDPR): Aantoonbaar inzicht hebben!

Het woord “aantoonbaar” speelt een belangrijke, cruciale rol in de nieuwe wetgeving.
Bedrijven en organisaties dienen volgens de nieuwe wetgeving aan de autoriteit te kunnen aantonen dat ze adequate technische- en organisatorische maatregelen hebben genomen om de bescherming en de privacy van de persoonsgegevens te waarborgen. Er moet inzicht zijn in de gegevensverwerkingen van de organisatie en de specifieke risico’s van die verwerkingen. Bij de aanwezigheid van privacy-risico’s dient er een plan van aanpak te zijn voor het nemen van maatregelen om deze risico’s te verlagen of te elimineren. Deze informatie dient beschikbaar te zijn middels een actueel bijgehouden privacy administratie.

Verplichtingen in de GDPR:

De GDPR legt de volgende verplichtingen op aan bedrijven en organisaties die persoonsgegevens verwerken:

- Documentatieplicht (Documenteren van alle verwerkingen van persoonsgegevens)
- Informatieplicht (Informeren van betrokkenen)
- Faciliteren rechten betrokkene
- Beveiligingsplicht (Adequaat beveiligingsniveau van verwerking van persoonsgegevens)
- Meldingsplicht (Meldplicht voor datalekken)

Om aan bovenstaande verplichtingen te kunnen voldoen is het noodzakelijk dat bedrijven de nodige voorbereidingen en maatregelen treffen. Dit betreft technische- en organisatorische maatregelen. Bij technische maatregelen moet worden gedacht aan bijvoorbeeld de ICT-inrichting en beveiliging en bij organisatorische maatregelen aan hoe daarmee wordt omgegaan (mensen en processen).

Meldplicht voor datalekken:

Incidenten waarbij persoonsgegevens toegankelijk worden voor onbevoegden moeten in de nieuwe wetgeving “onverwijld” (= binnen 72 uur!) worden gemeld aan de toezichthouder, de Autoriteit Persoonsgegevens. Een datalek kan onder andere ontstaan door een hackersaanval, een verloren USB-stick, laptop, tablet of smartphone, een fysieke inbraak, een verkeerd gestuurde email, etc. De melding aan de toezichthouder bevat een grote hoeveelheid gedetailleerde informatie zoals de aard van het datalek, hoe het is ontstaan, welke maatregelen er genomen worden, hoeveel betrokkenen, en in hoeverre er kans is op privacy schending van de betrokkenen. Indien er sprake is van mogelijke privacy schending voor de betrokkenen zal er ook een melding plaats moeten vinden aan alle betrokkenen.

Waar te beginnen?

Het begint met weten en bewustzijn:

De AVG heeft regelgeving over hoe omgegaan moet worden met persoonsgegevens. Niet zozeer "hoe" dat moet maar waaraan dit moet voldoen. Zoals de rechten van betrokkenen (mensen), de meldplicht datalekken en de afspraken die gemaakt moeten worden met externe verwerkers.
Een bedrijf moet de persoonsgegevens goed in kaart hebben (onder andere: welke zijn dat eigenlijk, waar en hoe lang worden deze bewaard, waar gebruiken we ze voor en welke rechtsgrond hebben we om deze gegevens te verwerken).
Iedereen die toegang heeft moet uiterste zorgvuldigheid voor de veiligheid van die gegevens toepassen (bijvoorbeeld: hoe doen de interne mensen dat, hoe bewust zijn we van de risico's, hoe doen externe verwerkers dat en hebben we afspraken vastgelegd).
Werkprocessen en techniek zo optimaal mogelijk inrichten (zoals: hebben we maatregelen getroffen om naar beste kunnen het risico op inbreuk op persoonsgegevens te voorkomen en hebben we processen ingericht om te kunnen voldoen aan een verzoek volgens de rechten die personen hebben volgens de AVG).

Het is nu voor de meesten van belang om de eerste stap in de inventarisatie te zetten; het verzamelen van informatie. Dit lijkt veelomvattend en complex maar een aantal tips maakt dat een stuk gemakkelijker. Daar kan TSD u bij ondersteunen.

Geïnteresseerd om door middel van tips gestructureerd uw informatie te gaan verzamelen?
Neem dan contact op met TSD.

Op basis van de verzamelde informatie kunt u een risico-inventarisatie uitvoeren of dit te laten doen door Sebyde door middel van een "quick-scan". U krijgt op verzoek kosteloos de privacy checklist aangeleverd die u kunt vullen met de door u verzamelde gegevens. Deze privacy checklist levert u aan bij Sebyde en deze wordt dan beoordeeld door specialisten. Naar aanleiding van deze beoordeling ontvangt u een rapportage over de eerste indruk van de privacy-situatie, de risico's en een advies over de te nemen stappen om aan de AVG/GDPR wetgeving te voldoen. Voor het beoordelen van een ingevulde Checklist en het maken van de rapportage brengt Sebyde € 495,= exclusief BTW in rekening.
Op basis van deze rapportage kunt u beslissen of u zich bij het maken van een plan en inrichten van maatregelen wilt laten ondersteunen. Sebyde kan u uitgebreid informeren over de mogelijkheden.

De Privacy Checklist van Sebyde is gratis aan te vragen via: https://www.sebydeprivacy.nl/rie-privacy/.

Sebyde BV – Sebyde Academy – Sebyde Privacy

Sebyde is een IT-security bedrijf gespecialiseerd in het verbeteren van de informatiebeveiliging van bedrijven en het vergroten van het bewustzijn van medewerkers op het gebied van de gevaren en risico's. Hierdoor wordt het aantal security-incidenten en datalekken sterk verlaagd. Vanuit Sebyde Privacy ondersteunen we bedrijven bij de voorbereiding op de AVG/GDPR wetgeving.

Met vragen is het uiteraard altijd mogelijk om contact met ons te zoeken.

Met vriendelijke groet,

Sebyde BV

Rob Koch
rob.koch@sebyde.nl
Tel: 06-53233269

Contact gegevens Sebyde BV

Sebyde BV

Telefoon: 085 - 2733376
Email: info@sebyde.nl

Website Sebyde Security: www.sebyde.nl
Website Sebyde Academy: www.sebydeacademy.nl
Website Sebyde Privacy: www.sebydeprivacy.nl

LinkedIn: www.linkedin.com/company/sebyde-bv
Twitter: www.twitter.com/SebydeBV
Facebook: www.facebook.com/sebydeBV