25 MEI 2018

DE GDPR

Een praktisch stappenplan

DE JURISTEN

PART OF THE JURISTS EUROPE

STARTBYTE

AUTOMATISERING

INHOUDSOPGAVE

01 INLEIDING

Vanaf 25 mei 2018 is de nieuwe Europese privacywetgeving rechtstreeks van toepassing in alle lidstaten van de Europese Unie. Deze ‘Algemene Verordening Gegevensbescherming’ (AVG) wordt ook wel de ‘General Data Protection Regulation’ (GDPR) genoemd. De AVG vervangt de huidige Nederlandse privacywetgeving, de Wet bescherming persoonsgegevens (Wbp). Met deze Europese regelgeving wordt de privacywetgeving in alle Europese landen nagenoeg gelijk getrokken.

Transparantie en accountability zijn de twee sleutelwoorden van de nieuwe wetgeving. Als organisatie word je verplicht open te zijn over de persoonsgegevens die je verzamelt en wat je daar mee doet. Daarnaast moet je kunnen aantonen dat jouw beveiligingsmaatregelen op orde zijn. Een datalek is nou eenmaal nooit voor 100% te voorkomen, daar gaat de wetgeving ook niet van uit. Maar mocht het dan toch gebeuren, dan moet je bij de nationale toezichthouder (Autoriteit Persoonsgegevens) kunnen aantonen dat jouw beveiliging en gegevensadministratie op orde zijn.

02

WANNEER IS DE GDPR VAN TOEPASSING?

De GDPR is van toepassing op iedere organisatie die persoonsgegevens verwerkt van personen die zich in de Europese Unie bevinden. Persoonsgegevens zijn alle gegevens die direct of indirect tot een persoon herleidbaar zijn, denk aan naam, adres en e-mail, maar ook IP-adressen, locatiegegevens, medische gegevens of bankgegevens. Bedrijfsgegevens zijn geen persoonsgegevens, maar persoonsgegevens van je werknemers wel. Er is sprake van 'verwerken' wanneer je gegevens verzamelt, vastlegt, ordent, opslaat, wijzigt, opvraagt, raadpleegt, gebruikt of wist. Kortom; de GDPR zal op vrijwel alle organisaties van toepassing zijn.

Niet iedere organisatie zal echter aan even strenge verplichtingen moet voldoen, dit hangt namelijk sterk af van de hoeveelheid persoonsgegevens die worden verwerkt. Daarnaast is het ook van belang om welke persoonsgegevens het gaat. Wanneer het bijvoorbeeld om gevoelige gegevens gaat, zoals medische gegevens, zullen de verplichtingen strenger worden en zullen (nog) meer voorzorgsmaatregelen getroffen moeten worden.

03

STAPPENPLAN

In deze brochure helpen wij je in 10 stappen op weg met de praktische toepassing van de nieuwe privacyregels op jouw organisatie.

Deze stappen hebben we opgedeeld in drie categorieën:

A . Organisatorische maatregelen: wat moet intern worden geregeld?

1. Creëer privacy bewustzijn binnen je organisatie en stel een intern beleid op
2. Stel een verwerkingsregister op
3. Beveiligingsmaatregelingen
4. De procedure na een datalek
5. Data Protection Officer (DPO)
6. Continue evaluatie

B . Verplichtingen richting je cliënten

7. Wees transparant over de persoonsgegevens die je verwerkt
8. Zorg dat je op basis van een correcte grondslag gegevens verwerkt
9. Rechten van betrokkenen

C . Afspraken met partners

10. Worden gegevens gedeeld? Maak duidelijke afspraken in een verwerkersovereenkomst

A

ORGANISATORISCHE MAATREGELEN

1. CREËER PRIVACY BEWUSTZIJN BINNEN JE ORGANISATIE EN STEL EEN INTERN BELEID OP OP.

Veel datalekken ontstaan door menselijk handelen. Denk aan een verloren usb-stick of een werknemer die toegang heeft tot gegevens waar hij of zij niet bij hoort te kunnen. Naast alle technische en organisatorische maatregelen, is het daarom ook van belang dat personen binnen een organisatie bewust gaan nadenken over gegevensbescherming en privacy. Zorg er daarom voor dat alle medewerkers op de hoogte zijn van het belang van gegevensbescherming en dat zij vervolgens op gepaste wijze omgaan met de verwerkte persoonsgegevens (zie ook paragraaf 4 voor enkele praktische tips). Een privacybeleid dat intern niet bekend is en niet wordt opgevolgd is namelijk zinloos.

Ook onderdeel van het interne privacybeleid zijn twee nieuwe termen die de GDPR introduceert, *'privacy by design'* en *'privacy by default.'*

Privacy by design betekent dat je in het ontwikkelproces al rekening houdt met de kernwaarden van privacybescherming en voldoende technisch en organisatorische maatregelen neemt. Verzamel als organisatie bijvoorbeeld niet meer persoonsgegevens dan noodzakelijk en pas vanaf de ontwikkelingsfase dataminimalisatie toe.

Ook bij bestaande processen is dit belangrijk en kan geëvalueerd worden welke data nu echt noodzakelijk zijn voor het leveren van een product of dienst. Privacy by default houdt in dat de standaardinstellingen altijd zo privacy vriendelijk mogelijk zijn. Men kan er dan vervolgens zelf voor kiezen om meer persoonlijke gegevens openbaar te maken. Denk hierbij bijvoorbeeld aan privacy vriendelijke browserinstellingen of de instellingen van een applicatie.

2. STEL EEN VERWERKINGSREGISTER OP

Een verwerkingsregister is bedoeld om duidelijk in kaart te brengen welke stromen van persoonsgegevens er binnenkomen en welke er uit een organisatie stromen. Voor organisaties van meer dan 250 werknemers is een verwerkingsregister verplicht. Voor organisaties met minder dan 250 werknemers, is een verwerkingsregister alleen verplicht indien er structureel persoonsgegevens worden verwerkt.

Toch zullen veel kleine organisaties ook aan deze plicht moeten voldoen, omdat in maar weinig gevallen echt incidenteel (een paar keer per jaar) persoonsgegevens worden verwerkt. Het opstellen van zo'n verwerkingsregister is natuurlijk een extra administratieve last. Anderzijds geeft het ook een duidelijk en georganiseerd overzicht van de datastromen in een organisatie.

Het opstellen van zo'n register is bovendien geen hogere wiskunde en kan in bijvoorbeeld Microsoft Excel worden opgesteld.

Per categorie persoonsgegevens die je verzamelt moet het volgende geregistreerd worden:

a. Wat voor soort persoonsgegevens worden er verzameld?
b. Wat is het doel van de gegevensverzameling?
c. Welke interne partijen (medewerkers) hebben toegang tot de gegevens?
d. Welke externe partijen hebben toegang tot de gegevens?
e. Waar worden de gegevens opgeslagen?
f. Wat zijn de (voorgenomen) bewaartermijnen?
g. Welke beveiligingsmaatregelen worden er genomen?

3. WELKE BEVEILIGINGSMAATREGELEN MOET IK NEMEN?

De wet geeft aan dat organisaties 'passende technische en organisatorische maatregelen' moeten nemen om persoonsgegevens te beschermen tegen verlies en onrechtmatige verwerking. De volgende voorbeelden worden in de wet genoemd:

1. Pseudonimisering en versleuteling van persoonsgegevens.
2. Maatregelen om de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van verwerkingssystemen en diensten te garanderen.
3. Maatregelen gericht op het tijdig kunnen herstellen van de beschikbaarheid van en de toegang tot persoonsgegevens bij een fysiek of technisch incident.
4. Het vaststellen van adequate procedures voor het periodiek evalueren van de doeltreffendheid van de genomen veiligheidsmaatregelen.

Echt specifieke beveiligingsverplichtingen zal je in de wet dus niet aantreffen. Je bent als organisatie ook zeker niet verplicht om voor iedere soort persoonsgegevens de allerzwaarste beveiligingsmaatregelen te nemen. Maatregelen moeten immers 'passend' zijn. E-mailadressen zal je dus minder goed hoeven te beveiligen dan bankrekeningnummers.

De wet noemt bovendien ook de omvang en financiële mogelijkheden van een organisatie als maatstaf. Van een kleine organisatie wordt niet verwacht dat zij een hypermodern beveiligingssysteem aanschaffen. Meer praktische beveiligingstips vind je aan het einde van deze brochure.

4. DE PROCEDURE NA EEN DATALEK

Een organisatie kan preventieve maatregelen nemen, maar er bestaat altijd een kans dat een datalek ontstaat als gevolg van een beveiligingsprobleem of als gevolg van menselijk handelen. Naast het preventieve beleid dat organisaties moeten voeren, moet er daarom ook rekening worden gehouden met het reactieve beleid. Moet een datalek altijd gemeld worden en aan wie?

Meldplicht voor de verwerkingsverantwoordelijke
Wanneer een datalek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen, moet dit bij de toezichthoudende instantie (in Nederland: de Autoriteit Persoonsgegevens) worden gemeld. Een melding aan de toezichthouder moet in ieder geval binnen 72 uur zijn gedaan nadat het datalek is ontdekt. Zorg er dus voor dat hier een procedure voor is opgesteld. Een melding moet de volgende informatie bevatten:

- De aard van de inbreuk;
- De instanties waar meer informatie over de inbreuk kan worden verkregen;
- De aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken;
- Een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens;
- De maatregelen die de organisatie heeft genomen of voorstelt te nemen om deze gevolgen te verhelpen.

Wanneer een datalek is ontstaan dat een hoog risico inhoudt voor de rechten en vrijheden van personen, dan zal dit datalek ook gemeld moeten worden aan de betrokkene(n) zelf. Tenzij, de verwerkingsverantwoordelijke passende technische beschermingsmaatregelen heeft genomen die de persoonsgegevens onbegrijpelijk of ontoegankelijk maken voor iedereen die geen recht op toegang heeft tot die gegevens. Denk hierbij bijvoorbeeld aan versleutelde gegevens die niet door derden kunnen worden gelezen.

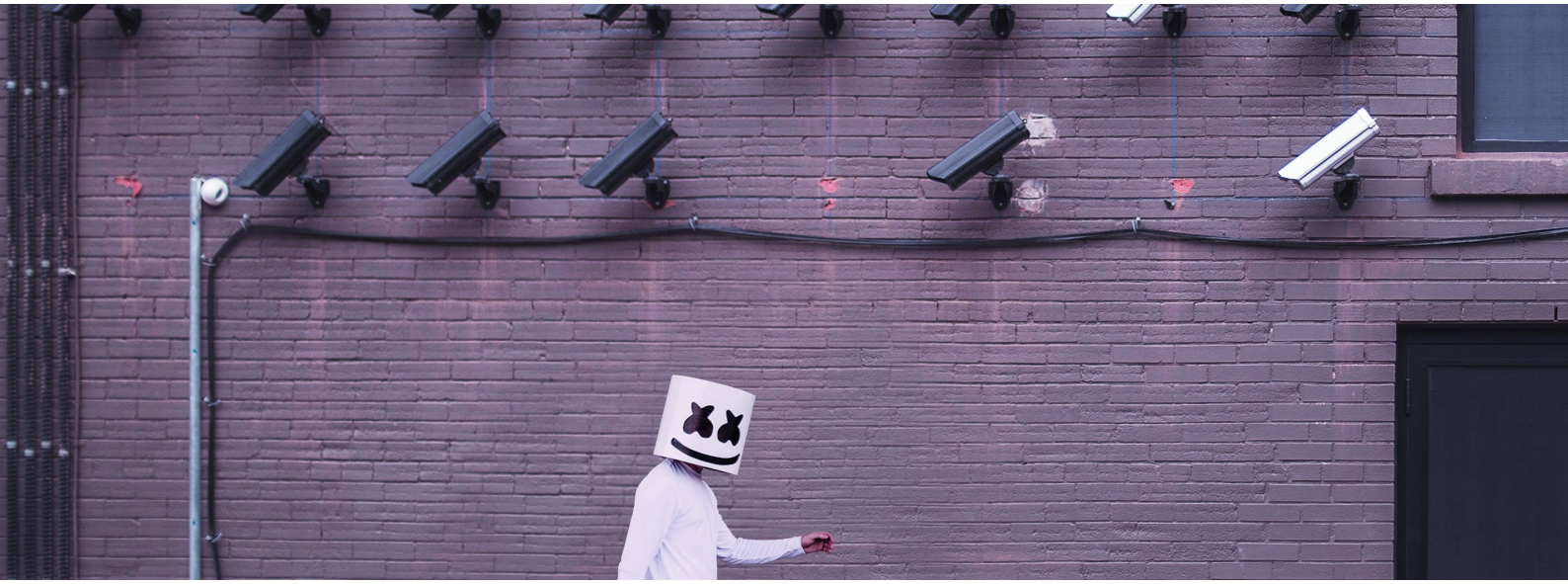
Meldplicht voor de verwerker
Een datalek kan ook ontstaan bij de verwerker, die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Een verwerker is verplicht ieder datalek te melden aan de verwerkingsverantwoordelijke. Afhankelijk van de contractuele afspraken tussen de verwerker en verwerkingsverantwoordelijke, meldt de verwerker het datalek ook bij de toezichthoudende autoriteit of betrokkenen.

5. DATA PROTECTION OFFICER (DPO)

De taak van een DPO is het toezien op de bescherming van verwerking van persoonsgegevens binnen de organisatie en naleving van de relevante wetgeving. De DPO is aanspreekpunt binnen de organisatie, voor betrokkenen en toezichthouders. Een DPO kan een personeelslid zijn, of een externe persoon of organisatie. Een parttime of fulltime functie zijn beide mogelijk. De aanstelling van een DPO is verplicht indien een organisatie één van de volgende kernactiviteiten op grote schaal uitvoert:

1. Regelmatig of stelselmatig personen observeren.
2. Bijzondere persoonsgegevens verwerken: hieronder vallen gezondheid, ras, politieke opvattingen, geloofsovertuiging en strafrechtelijk verleden.
3. Daarnaast is een DPO verplicht voor iedere overheidsinstantie of overheidsorgaan.

Buiten overheidsinstanties, zal je als organisatie lang niet altijd een DPO hoeven in te stellen. Dit is enkel noodzakelijk indien je gevoelige gegevens verwerkt of indien stelselmatig personen worden gevolgd. Denk hierbij o.a. aan profilering, dus het analyseren en combineren van persoonsgegevens om iemand zo in een bepaalde categorie te kunnen indelen. Bijvoorbeeld wifi-tracking, risico analyses, cameratoezicht en slimme meters.



6. EVALUATIE

Een organisatie zal niet van de ene op de andere dag volledig GDPR compliant zijn. Het is dan ook vooral belangrijk dat het proces in gang wordt gezet en dat na verloop van tijd alle nodige stappen zijn gezet. Uiteindelijk zal het privacy beleid deel moeten gaan uitmaken van het grotere geheel en zal dit continue verbeterd dienen te worden.

B

VERPLICHTINGEN RICHTING JE CLIËNTEN

7. WEES TRANSPARANT OVER DE PERSOONSGEGEVENS DIE JE VAN MENSEN VERWERKT

Als organisatie dien je transparant te zijn tegenover de personen waarvan je gegevens verzamelt (de betrokkenen) en waarom die verzameld worden. De meest gangbare manier om klanten hierover te informeren is via een apart privacybeleid (privacy policy) dat voor betrokkenen gemakkelijk te raadplegen is. Bijvoorbeeld via de website van jouw organisatie of via een correcte privacy clausule bij het aangaan van een overeenkomst. Een privacybeleid moet in heldere taal geschreven worden, geen juridisch jargon dus. Het moet in ieder geval de volgende informatie bevatten:

1. Welke persoonsgegevens er verzameld worden.
2. Het doel waarvoor de persoonsgegevens verzameld worden (de grondslag).
3. Informatie over de wijze van inzage, correctie of verwijdering van persoonsgegevens.
4. De bewaartermijn van gegevens.
5. Categorie van derde partijen waar persoonsgegevens mee worden gedeeld.
6. Contactgegevens van de eigen organisatie.

8. ZORG DAT JE OP BASIS VAN EEN CORRECTE GRONDSLAG GEGEVENS VERWERKT

Op basis van de oude Nederlandse privacywetgeving waren er een aantal grondslagen op basis waarvan je persoonsgegevens mocht verwerken. Die grondslagen zijn grotendeels overgenomen. Organisaties verwerken rechtmatig gegevens indien voldaan is aan één van de onderstaande zes voorwaarden:

Meest voorkomende grondslagen:

1. De verwerking is noodzakelijk voor de uitvoering van de overeenkomst.
2. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting.
3. De verwerking is op basis van een gerechtvaardigd belang van de verwerker of een derde.
4. De persoon heeft toestemming gegeven voor de verwerking.

Handelingen van overheidsorganen of situatie van leven of dood:

5. De verwerking is noodzakelijk voor de uitvoering van een taak van algemeen belang of uitoefening van het openbaar gezag.
6. De verwerking is noodzakelijk om de vitale belangen van de persoon te beschermen.

Voor commerciële organisaties zal de verwerking van persoonsgegevens in de meeste gevallen gebaseerd zijn op de eerste vier voorwaarden. Een voorbeeld van verwerking van persoonsgegevens die noodzakelijk zijn voor een overeenkomst, is een arbeidsrelatie. Indien een organisatie de salarisadministratie heeft uitbesteed aan een derde partij, dan zal die partij gegevens van werknemers ontvangen omdat dit nu eenmaal noodzakelijk is. Bij verwerking op grond van een wettelijke verplichting kun je denken aan de plicht tot loonaangifte of andere belastingen en premies.

Wat is nu een gerechtvaardigd belang van een organisatie? Dat zijn in ieder geval de verwerkingen die noodzakelijk zijn om reguliere bedrijfsactiviteiten te verrichten. Daarbij hoort bijvoorbeeld ook direct marketing, intern marktonderzoek en de bestrijding van fraude. Verder is deze grondslag deels een open norm. Als organisatie zal je je moeten afvragen of er bij de verwerking van persoonsgegevens geen fundamentele rechten van personen geschonden worden.

Toestemming wordt veel gebruikt als grondslag, maar is eigenlijk de meest zwakke grond. Toestemming vragen voor verwerking betekent dat de andere grondslagen niet gebruikt kunnen worden. In dat geval zal een organisatie extra goed moet uitleggen waarom verwerking toch nodig is. Probeer daarom altijd eerst te kijken naar de mogelijkheden om de gewenste verwerking op andere grondslagen te baseren.

9. MAAK CORRECTIE, VERWIJDERING EN OPVRAGEN VAN GEGEVENS MOGELIJK

Personen moeten de mogelijkheid hebben om hun eigen gegevens te corrigeren en te verwijderen. Organisaties moeten duidelijk communiceren hoe dit gedaan kan worden. Je kunt dit automatiseren, maar duidelijke contactgegevens (e-mail) waar zo'n verzoek naartoe gestuurd kan worden volstaat ook.

Daarnaast moeten personen ook de mogelijkheid hebben om hun data op te vragen, ook wel dataportabiliteit genoemd. Wanneer je zo'n verzoek krijgt, moet je als organisatie de persoonsgegevens binnen een maand in een gangbare vorm opsturen. Dit kan bijvoorbeeld een Excelbestand zijn. Persoonsgegevens waarvan een organisatie wettelijk verplicht is om te bewaren, hoeven niet verwijderd te worden.

C

AFSPRAKEN MET PARTNERS

10. WORDEN GEGEVENS GEDEELD? MAAK DUIDELIJKE AFSPRAKEN IN EEN VERWERKERSOVEREENKOMST

Bijna iedere organisatie zal bepaalde persoonsgegevens delen met een derde partij. Ook kan het zo zijn dat je als organisatie zelf gegevens verwerkt van een andere partij. Afspraken over die verwerking van gegevens moeten verplicht vastgelegd worden in een zogenaamde '**verwerkersovereenkomst**'.

De verwerkersovereenkomst geeft inzicht in de verplichtingen en verantwoordelijkheden van beide partijen. Het doel van een verwerkersovereenkomst is dan ook om ervoor te zorgen dat verwerkers ook de nodige beveiligingsmaatregelen nemen. De onderstaande zaken moeten in ieder geval in een verwerkersovereenkomst opgenomen zijn:

1. De duur, beschrijving en doeleinden van de gegevensverwerking.
2. Beveiligingsmaatregelen en audits.
3. Waarborging van betrouwbaarheid van personeel.
4. Melding van een datalek aan verwerkingsverantwoordelijke.
5. Medewerkings- en inlichtingenplicht.
6. Toestemming voor inschakelen subverwerkers.
7. Waarborgen bij gegevensverkeer buiten de EU.
8. Retour of vernietiging van gegevens bij einde van de dienstverlening.

04

PRAKTISCHE TIPS:

Hieronder vind je enkele praktische tips op organisatorisch en technisch vlak die gemakkelijk zijn door te voeren. Een aantal tips zijn open deuren, er wordt echter niet altijd bij stil gestaan.

• Houd je software up-to-date, gebruik antivirus software, schakel je firewall in en stel automatische schermvergrendeling in voor computers. Simpele aandachtspunten die vaak vergeten worden door gewoonte of laksheid.

• Gebruik een spamfilter en schakel 'remote content' uit. Door remote content uit te schakelen worden bijlages niet automatisch gedownload wanneer je een e-mail opent. Zo kunnen spammers niet zien dat de e-mail is geopend en dat je dus actief bent op dat e-mailadres.

• Gebruik zo min mogelijk mobiele gegevensdragers zoals usb-sticks. Oké, gebruik ze eigenlijk gewoon niet. Doe je het toch? Zorg er dan voor dat jouw mobiele gegevensdrager beveiligd is.

• Zorg voor sterke authenticatie. Gebruik sterke wachtwoorden of gebruik bij gevoelige gegevens twee-factor authenticatie (een tweede controle naast een wachtwoord).

• Zorg voor periodieke online of offline back-up systemen. Idealiter met encryptie en data-opslag binnen Europa.

• Versleutel data daar waar dit mogelijk is. Denk bijvoorbeeld aan end-to-end-encryptie van harde schijven en clouddiensten.

• Beperk de toegang tot persoonsgegevens. Sla verschillende soorten persoonsgegevens op verschillende niveaus op en geef enkel toegang aan personen die inzage in de gegevens nodig hebben voor de uitoefening van hun werkzaamheden. Check daarnaast of de (arbeids)overeenkomsten van medewerkers die toegang hebben tot persoonsgegevens een sluitend geheimhoudingsbeding bevatten.

• Zorg voor fysieke beveiliging van gegevens. Heb je als organisatie eigen servers? Zorg dan dat deze achter slot en grendel staan, evenals papieren dossiers die persoonsgegevens bevatten.

• Houd toezicht. Maatregelen nemen en een intern privacybeleid opstellen is één ding. De volgende stap is dat medewerkers bewust worden (en blijven) van informatieveiligheid en dat er adequaat toezicht gehouden wordt op de naleving van eigen protocollen en de wet- en regelgeving.

WAT KAN DEJURISTEN VOOR JOUW ORGANISTIE BETEKENEN?

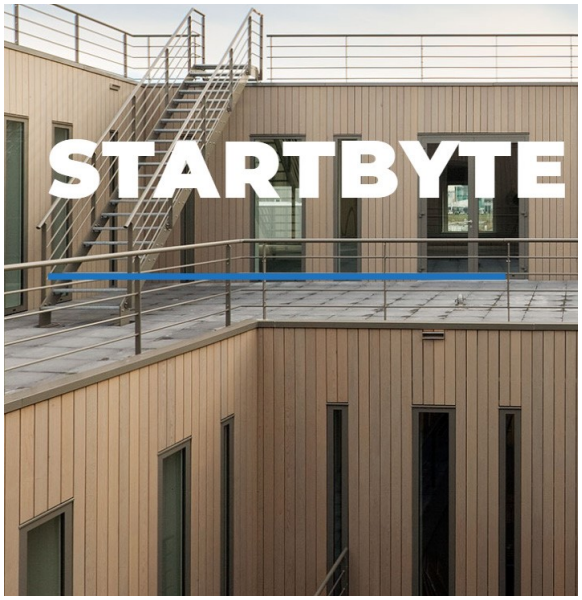
deJuristen helpt jouw organisatie privacy compliant te worden op juridisch en organisatorisch vlak. Eerst voeren wij een privacy audit uit, zo wordt het voor ons duidelijk op welke punten een organisatie zich moet verbeteren. Ben je een grote organisatie, dan gebruiken wij hier een softwaretool voor.

Aan de hand van de audit stellen wij een actieplan op en bespreken wij met jou welke maatregelen er genomen moeten worden.

WAT KAN STARTBYTE VOOR JOUW ORGANISTIE BETEKENEN?

Startbyte biedt een oplossing voor bedrijven die te klein zijn voor een eigen fulltime ICT-medewerker, maar hier wel behoefte aan hebben. In samenwerking met jouw organisatie helpt Startbyte om de technische maatregelen te nemen die nodig zijn onder de GDPR.

Een voorbeeld van zo'n technische maatregel is cybersensor 'SAM'. Dit is een klein apparaat dat aan een netwerk wordt geschakeld. Zo krijg je bij onraad (bijvoorbeeld installatie van malware) direct een melding per e- mail of sms. Doordat Startbyte deze dienst heeft geautomatiseerd, heb je alle voordelen van professionele (en dure) security monitoring zonder de bijbehorende hoge kosten.



CONTACT

deJuristen Amsterdam

Adres: Johan Huizingalaan 763A, 1066 VH Amsterdam, Nederland.

Telefoon: (+31) 085 888 3900

Email: contact@dejuristen.legal

Startbyte

Adres: T.T. Vasumweg 154, 1033 SH Amsterdam, Nederland.

Telefoon: (+31) 20 845 7676

Email: info@startbyte.nl