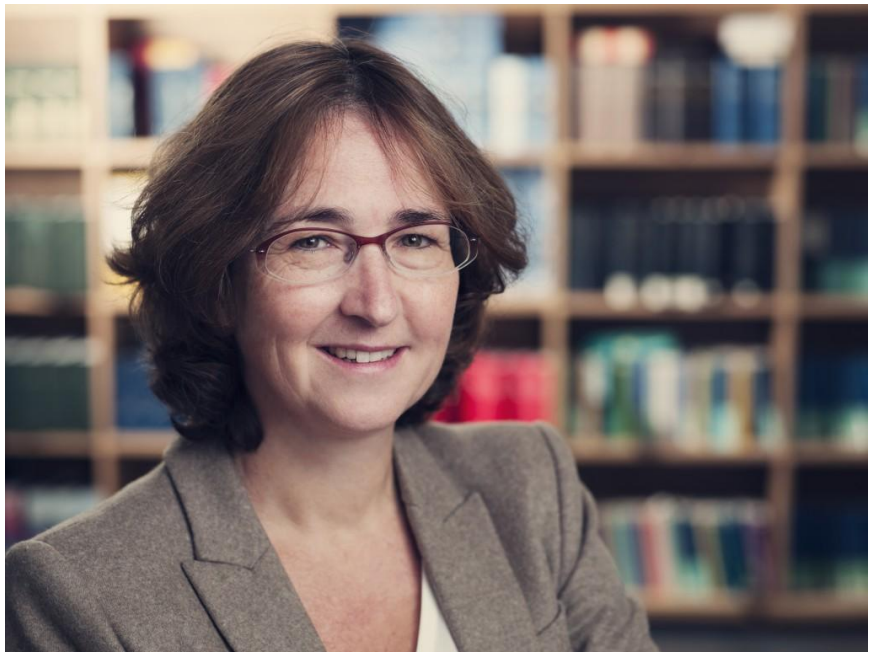
POT JONKER advocaten

Cursus Privacy & AVG Sport Support

16 april 2018

Haarlem



Anke van de Laar
vandelaar@potjonker.nl
023-5530233

Michael Reker
reker@potjonker.nl
023-5530263

Programma

- Quiz
- Hoofdbeginselen van privacyrecht
- Stappenplan

QUIZ

Vraag 1

- Is uw organisatie al begonnen met de voorbereiding op het van kracht worden van de Algemene Verordening Gegevensbescherming (AVG) per 25 mei 2018?

- *Ja / Nee / Te weinig / Geen idee*

Vraag 2

- Is er in uw organisatie budget beschikbaar gesteld voor de implementatie van de AVG?

- *Ja / Nee / Te weinig / Geen idee*

Vraag 3

- Is uw organisatie op tijd klaar om per 25 mei 2018 te voldoen aan de AVG?

- *Ja / Nee / Nee, maar goed op weg / Geen idee*

Vraag 4

- U voegt thuis de naam en contactgegevens van een vriend toe aan de map ‘adressenbestand’ op uw pc. Is sprake van een verwerking van persoonsgegevens?

- *Ja of nee?*

Vraag 5

- Het bestuur van uw organisatie maakt per e-mail aan alle leden en/of vrijwilligers bekend dat bestuurslid X onverwacht is overleden als gevolg van een hartaanval. Mag dat op grond van privacyregelgeving?

- *Ja of nee?*

Vraag 6

- Uw organisatie vraagt (onbetaalde) vrijwilligers om bij hun aanmelding een kopie van hun identiteitsbewijs te overleggen. Mag dat?

- *Ja of nee?*

Vraag 7

- U meldt zich aan als lid van de plaatselijke boogschuttersvereniging want de contributie is niet hoog. De vereniging neemt vervolgens uw gegevens op in hun administratie. Is daarvoor uw toestemming nodig?

- *Ja of nee?*

Vraag 8

- U bent al jarenlang vrijwilliger bij het dierenasiel. Als gevolg van gezondheidsproblemen lukt het u niet meer om als vrijwilliger aan de slag te blijven en u meldt zich af. Het dierenasiel bewaart uw gegevens nog 5 jaar. Mag dat?

- *Ja of nee?*

Vraag 9

- Uw organisatie gaat met de tijd mee. Uw vrijwilligersbestand staat opgeslagen in de cloud. Moet u met de cloudprovider afspraken maken over privacy?

- *Ja of nee?*

Vraag 10

- De plaatselijke voetbalvereniging heeft op een afgeschermd deel van haar website dat alleen toegankelijk is voor leden, van elk lid een foto en de naam opgenomen, gerangschikt per team. De algemene ledenvergadering heeft ingestemd met deze werkwijze. Is daarnaast van elk lid afzonderlijk toestemming vereist?

- *Ja of nee?*

Vraag 11

- Uw organisatie heeft de beveiliging van persoonsgegevens op orde. Toch trapt één van de medewerkers in een phishing mail waarna ransomware op zijn computer wordt geïnstalleerd. Is dit een datalek?

- *Ja of nee?*

HOOFDBEGINSELEN VAN PRIVACYRECHT

Hoofdbeginselen privacyrecht (1/2)

- Ga zorgvuldig met persoonsgegevens om
- Zorg dat de gegevens die je verwerkt juist zijn
- Zorg dat de verwerking rechtmatig is (is er een grondslag?)
- Verwerk persoonsgegevens alleen voor uitdrukkelijk omschreven doelen
- Verwerk niet meer gegevens dan noodzakelijk

Hoofdbeginselen privacyrecht (2/2)

- Verwerk persoonsgegevens niet op een manier die niet verenigbaar is met de doeleinden waarvoor je ze hebt verkregen
- Zorg dat het doel en middel in verhouding zijn (proportionaliteit & subsidiariteit)
- Informeer de betrokkene over de verwerking (rechten!)
- Bewaar de gegevens niet langer dan nodig is
- Laat zien dat je voldoet aan de AVG (verantwoordingsplicht)

STAPPENPLAN

Stappenplan

- Stap 1: Bewustwording
- Stap 2: Maak iemand verantwoordelijk
- Stap 3: Inventariseer welke gegevens worden verwerkt en zet dit in een register
- Stap 4: Beveilig de gegevens
- Stap 5: Sluit zo nodig verwerkersovereenkomsten
- Stap 6: Informeer de betrokkenen (privacyverklaring)
- Stap 7: Stel (interne) protocollen op

Stap 1: Bewustwording

- Zorg dat de mensen in uw organisatie zich bewust zijn van het feit dat ze persoonsgegevens verwerken.

- Wijs ze op de risico's:
  - Reputatieschade
  - Verlies aan vertrouwen
  - Hoge boetes

Stap 2: Beleg verantwoordelijkheid

- Maak iemand verantwoordelijk in de organisatie
  - Indien mogelijk, stel een werkgroep samen
  - In de werkgroep ook een lid van het bestuur/directie

- Functionaris gegevensbescherming (interne toezichthouder) o.m. verplicht voor organisaties die vanuit hun kernactiviteiten op grote schaal bijzondere persoonsgegevens verwerken

- Budget?

Stap 3: Inventariseer (1/3)

- Ga na welke gegevens worden verwerkt in de organisatie
  - Gegevens van vrijwilligers / medewerkers / cliënten / andere betrokkenen (bv. familieleden)
  - NAWTE-gegevens / medische gegevens (allergie-informatie, medicijngebruik) / foto's
  - Gegevens van ontvangers (vrijwilligers, ingeschakelde derden)
- Voor welk doel worden deze gegevens verwerkt?
  - Bijhouden ledenadministratie, leveranciers, oud-leden
- Hoe lang worden de gegevens bewaard?

Stap 3: Inventariseer (2/3)

- Maak een register als sprake is van structurele verwerking
  - Vormvrij, wel schriftelijk (excelsheet, soms A4)

- Zet daarin voor elke verwerking:

  - de informatie die je hebt geïnventariseerd; en
  - de naam en contactgegevens van de organisatie (ook FG)
  - welke grondslag er is voor de verwerking (overeenkomst, gerechtvaardigd belang, wettelijke plicht, toestemming)
  - welke beveiligingsmaatregelen er zijn genomen

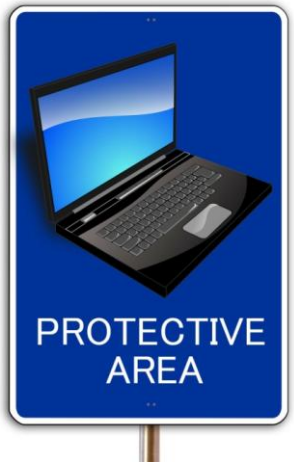
Stap 3: Inventariseer (3/3)

Naam verwerking	Administratie vrijwilligers
Naam en de contactgegevens	Vrijwilligersstichting Vrijwilligersstraat 1, Haarlem
Verwerkingsdoeleinden	Betalen onkostenvergoeding
Beschrijving van de categorieën van betrokkenen	Vrijwilligers
Beschrijving van de categorieën van persoonsgegevens	NAW-gegevens, bankrekeningnummer
Categorieën van ontvangers	Boekhouding, externe salarisadministratie
Bewaartermijnen	Twee jaar na beëindiging relatie
Algemene beschrijving technische en organisatorische beveiligingsmaatregelen	Fysieke toegangscontrole, logging, firewalls, versleutelde database/bestand
Grondslag verwerking	Uitvoering (vrijwilligers)overeenkomst

Stap 4: Beveilig (1/2)

- Tref passende technische en organisatorische maatregelen om persoonsgegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking, onopzettelijk verlies, vernietiging en/of beschadiging.

- Voorbeelden:
  - afschermen deel van de website
  - geheimhoudingsverklaringen met vrijwilligers
  - beveilig computers met wachtwoord
  - doe kast met gegevens op slot



Stap 4: Beveilig (2/2)

Autoriteit Persoonsgegevens lekte per ongeluk namen van personeel

De Autoriteit Persoonsgegevens, waarbij bedrijven datalekken verplicht moeten melden, heeft zelf per ongeluk de namen van werknemers openbaar gemaakt.

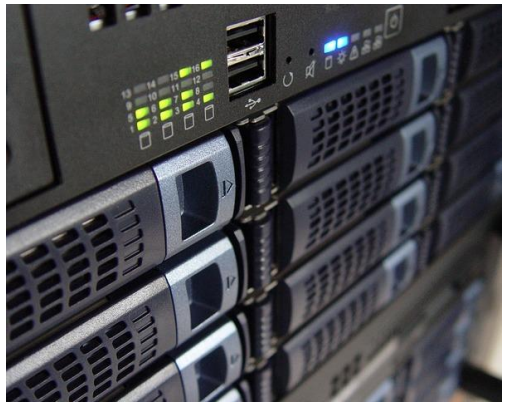
- Datalekken: inbreuk op de beveiliging (overgrote deel menselijke fouten -> bewustwording)
- Melden aan AP en eventueel betrokkene. Binnen 72 uur. Hoe melden? Digitaal via het meldloket datalekken van de AP https://datalekken.autoriteitpersoonsgegevens.nl
- Registreer de feiten, de gevolgen en de getroffen maatregelen

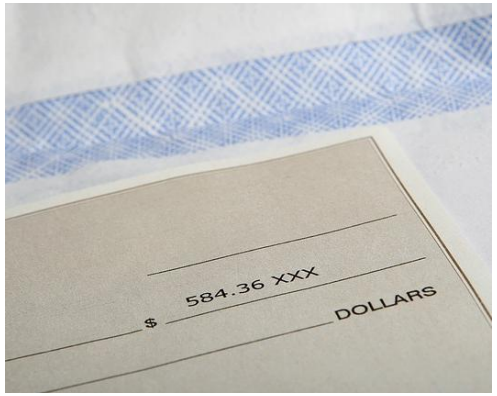
Stap 4: Datalek of niet?

- Vrijwilliger laat per ongeluk een laptop/iPad met daarop persoonsgegevens achter in een restaurant.
- USB-stick met daarop persoonsgegevens valt in het water en is niet meer uit te lezen.
- Een medewerker verstuurt de nieuwsbrief per e-mail en zet per ongeluk alle geadresseerden onder ‘aan’ i.p.v. onder ‘bcc’.
- Stukken met persoonsgegevens belanden in een vuilniszak op straat.

Stap 5: Verwerkersovereenkomst

- Verwerker: een natuurlijke persoon of rechtspersoon die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.
- Ga na wie uw organisatie inschakelt om gegevens te verwerken
  - bv. Cloudproviders, online ledenadministratie
- Let op met overeenkomsten van internet plukken. Verschillend perspectief verwerkingsverantwoordelijke/verwerker.





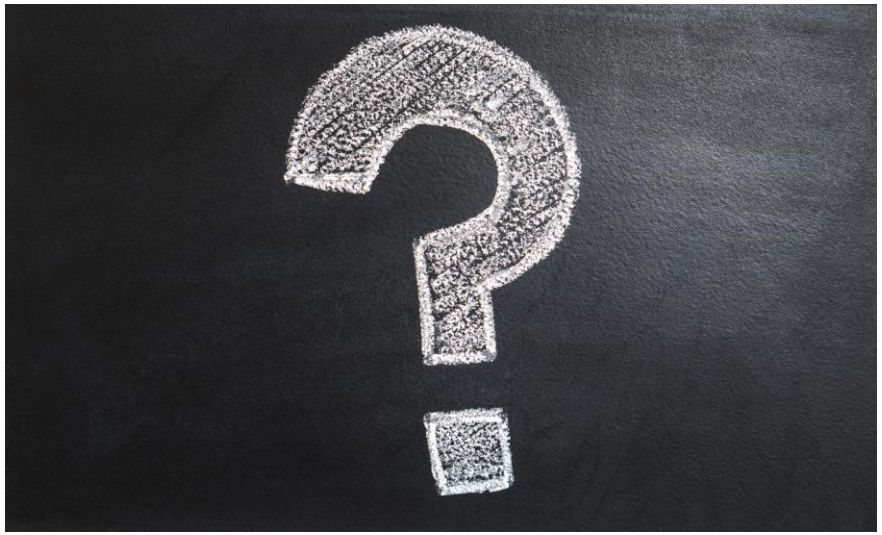
Stap 6: Informeer

- Informeer betrokkenen over de gegevensverwerkingen
- Hoe: privacyverklaring (flyer, website)
- Waarover:
  - alle informatie uit het register
  - uitoefenen privacyrechten: inzage, correctie, verwijdering, verzet, overdraagbaarheid

Stap 7: Intern beleid/Protocollen

- Vastleggen intern beleid rondom privacy
- Waarom: interne transparantie, eenduidige uitvoering
- Hoe: Maak intern protocollen zodat men weet wat te doen ingeval van bv:
  - Datalekken
  - Verzoeken van betrokkenen
  - Vertrek vrijwilligers
  - Naleven bewaartermijnen
  - Bring your own device (BYOD)

Vragen?



Anke van de Laar / Michael Reker
E vandelaar@potjonker.nl / reker@potjonker.nl
T +31 (0)23 55 30 233 / 263