Databescherming 2.0 –

Beginselen van de Algemene Verordening Gegevensbescherming: Bereid je voor in 13 stappen

CBPL
Commissie voor de bescherming van de persoonlijke levenssfeer

CPVP
Commission de la protection de la vie privée

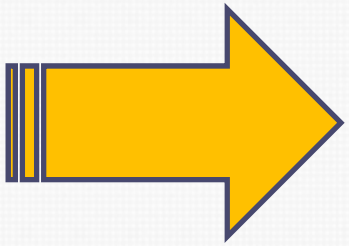
ASP
Ausschuss für den Schutz des Privatlebens

CPP
Commission for the protection of privacy

Caroline De Geest

18/09/2017

Introductie



Beginselen verwerking van persoonsgegevens (Art. 5)

Rechtmatig, behoorlijk en transparant

Doelbinding

Data minimalisatie

Juistheid

Opslag beperking

Integriteit & vertrouwelijkheid

NEW!
Verantwoordingsplicht

Rechtmatig, behoorlijk en transparant

- Gerechtvaardigde verwerkingsgrond
- Eerlijke, niet frauduleuse verwerking
- Informatie aan de betrokkene
  - Duidelijke taal
  - Regels, risico's en rechten

Doelbinding

- Welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden
- Geen verwerking op een manier die onverenigbaar is met die doeleinden

Data minimalisatie & juistheid

- Toereikend, ter zake dienend en beperkt tot wat noodzakelijk is voor het doeleinde waarvoor de gegevens worden verwerkt
- Verwerk dus enkel het strikte minimum
- De gegevens moeten accuraat zijn

Opslagbeperking

De gegevens mogen niet langer worden bewaard dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor zij worden verwerkt

Integriteit en vertrouwelijkheid

- Verwerking volgens afdoend veiligheidsniveau door gebruik te maken van passende, technische en organisatorische maatregelen
- Bescherming tegen iedere niet toegelaten of onwettige verwerking, tegen verlies, vernietiging of kwaliteitsverlies van de gegevens

Verplichtingen verantwoordelijke voor de verwerking

« Verantwoordingsplicht »

No “one-size-fits-all” approach

In praktijk – 13 stappen…

COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER
COMMISSION DE LA PROTECTION DE LA VIE PRIVEE

BEREID JE VOOR IN 13 STAPPEN

1. BEWUSTMAKING

Informeer sleutelfiguren en beleidsmakers over de aankomende veranderingen. Zij moeten inschatten welke gevolgen de AVG zal teweegbrengen voor het bedrijf of de organisatie.

2. DATAREGISTER

Breng in kaart welke persoonsgegevens je bijhoudt, waar deze vandaan komen en met wie je deze hebt gedeeld. Registreer je verwerkingen. Mogelijks dien je hiervoor een informatie-audit te organiseren.

3. COMMUNICATIE

Evalueer je bestaande privacyverklaring en plan noodzakelijke wijzigingen hieraan in het licht van de AVG.

4. RECHTEN VAN DE BETROKKENE

Ga na of de huidige procedures in je bedrijf of organisatie alle rechten voorzien waarop de betrokkene zich kan beroepen, inclusief hoe persoonsgegevens kunnen worden verwijderd of hoe gegevens elektronisch zullen worden meegedeeld.

5. VERZOEK TOT TOEGANG

Update je bestaande toegangsprocedures en bedenk hoe je verzoeken tot toegang voortaan zal behandelen onder de nieuwe termijnen in de AVG.

6. WETTELIJKE GRONDSLAG VOOR HET VERWERKEN VAN PERSOONSGEGEVENS

Documenteer de verscheidene types van gegevensverwerkingen die je uitvoert en identificeer de wettelijke grondslag voor elk van hen.

7. TOESTEMMING

Evalueer de wijze waarop je toestemming vraagt, verkrijgt en registreert, en wijzig waar nodig.

8. KINDEREN

Ontwikkel systemen die de leeftijd van de betrokkene nagaan en die de ouder(s) of voogdijen) om toestemming vragen voor de gegevensverwerking van minderjarige kinderen.

9. DATALEKKEN

Voorzie adequate procedures om persoonlijke datalekken op te sporen, te rapporteren en te onderzoeken.

10. GEGEVENSBESCHERMING DOOR ONTWERP EN GEGEVENSBESCHERMINGSEFFECTBEOORDELING

Maak je vertrouwd met de begrippen "gegevensbescherming door ontwerp" en "gegevensbeschermingseffectbeoordeling" en ga na hoe je deze concepten in de werking van jouw bedrijf of organisatie kan implementeren.

11. FUNCTIONARIS VOOR GEGEVENSBESCHERMING

Duid, indien nodig, een functionaris voor gegevensbescherming aan, of iemand die de verantwoordelijkheid draagt voor het naleven van de databeschermingsregels. Beoordeel welke plaats deze inneemt binnen de structuur en het beleid van jouw bedrijf of organisatie.

12. INTERNATIONAAL

Bepaal onder welke toezichthoudende autoriteit je valt indien jouw bedrijf of organisatie internationaal actief is.

13. BESTAANDE CONTRACTEN

Beoordeel je bestaande contracten, hoofdzakelijk met verwerkers en onderaannemers, en breng tijdig de noodzakelijke veranderingen aan.

In praktijk – 13 stappen…

1. BEWUSTMAKING

Informeer sleutelfiguren en beleidsmakers over de aankomende veranderingen. Zij moeten inschatten welke gevolgen de AVG zal teweegbrengen voor het bedrijf of de organisatie.

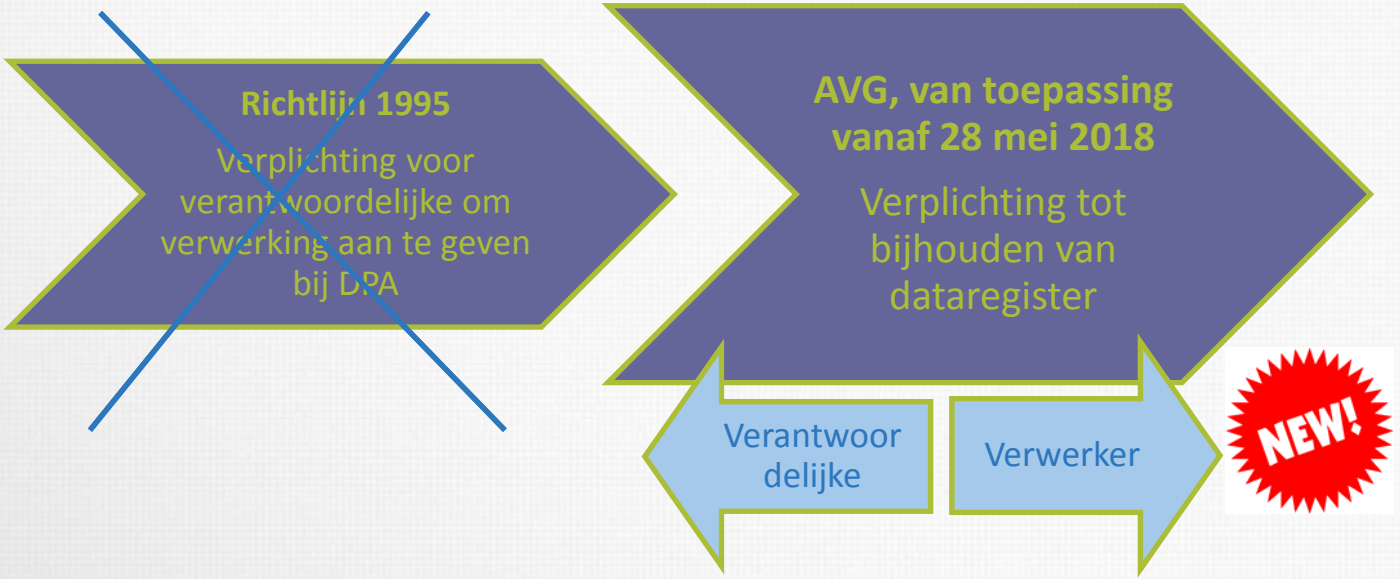
3. COMMUNICATIE

Evalueer je bestaande privacyverklaring en plan noodzakelijke wijzigingen hieraan in het licht van de AVG.

In praktijk – 13 stappen…

2. DATAREGISTER

Breng in kaart welke persoonsgegevens je bijhoudt, waar deze vandaan komen en met wie je deze hebt gedeeld. Registreer je verwerkingen. Mogelijks dien je hiervoor een informatie-audit te organiseren.



Dataregister

- ✓ Uitzondering voor KMO's (onderneming met minder dan 250 werknemers)

- ✓ Deze zijn hieraan a priori niet onderworpen behalve in drie gevallen:
  - de verwerking die zij verrichten houdt een risico in
  - de verwerking is niet incidenteel
  - de verwerking betreft gevoelige gegevens

- ✓ Aanbeveling uit eigen beweging 06/2017 + modelregister

Dataregister

WIE ?

- Vul de naam en de contactgegevens in van de verwerkingsverantwoordelijke (en zijn wettelijke vertegenwoordiger) en van de functionaris voor gegevensbescherming als u er een moet aanstellen

- Stel een lijst op van de verwerkers

WAT?

- Identificeer de categorieën verwerkte gegevens en de categorieën betrokken personen.
- Identificeer de zogenaamde gevoelige gegevens zoals de gezondheidsgegevens en gerechtelijke gegevens.

WAAROM?

Identificeer de doeleinden waarvoor de gegevens worden ingezameld. Er moet een beschrijving gebeuren per doeleinde.

WAAR?

- Vermeld de categorieën bestemmelingen (ook indien ze in derde landen gevestigd zijn) naar waar de gegevens worden overgedragen.
- Vermeld de doorgiften aan een derde land of internationale organisatie en identificeer het land en in voorkomend geval de bestaande passende waarborgen.

TOT WANNEER?

Vermeld voor iedere categorie gegevens de bewaartermijn. De bewaartermijn moet niet noodzakelijk uitgedrukt worden in aantal dagen, maanden of jaren maar mag ook verwijzen naar de tijd die noodzakelijk is om een concreet project te realiseren.

HOE?

Geef een algemene beschrijving van de ingevoerde technische en organisatorische beveiligingsmaatregelen die garanderen dat het beveiligingsniveau aan het risico is aangepast.

In praktijk – 13 stappen…

4. RECHTEN VAN DE BETROKKENE

Ga na of de huidige procedures in je bedrijf of organisatie alle rechten voorzien waarop de betrokkene zich kan beroepen, inclusief hoe persoonsgegevens kunnen worden verwijderd of hoe gegevens elektronisch zullen worden meegedeeld.

5. VERZOEK TOT TOEGANG

Update je bestaande toegangsprocedures en bedenk hoe je verzoeken tot toegang voortaan zal behandelen onder de nieuwe termijnen in de AVG.

- ✓ Transparantie en modaliteiten voor de uitoefening van de rechten
- ✓ Informatie en toegang tot persoonsgegevens
- ✓ Recht op verbetering en wissing
- ✓ Recht op de beperking van de verwerking
- ✓ Recht op bezwaar en geautomatiseerde besluitvorming, inclusief profiling

- ✓ NIEUW! Recht op overdraagbaarheid van gegevens

In praktijk – 13 stappen…

6. WETTELIJKE GRONDSLAG VOOR HET VERWERKEN VAN PERSOONSGEGEVENS

Documenteer de verscheidene types van gegevensverwerkingen die je uitvoert en identificeer de wettelijke grondslag voor elk van hen.

- ✓ Gerechtvaardigde verwerkingsgrond
- ✓ Eerlijke, niet frauduleuse verwerking
- ✓ Informatie aan de betrokkene
  - Duidelijke taal
  - Regels, risico's en rechten

In praktijk – 13 stappen…

7. TOESTEMMING

Evalueer de wijze waarop je toestemming vraagt, verkrijgt en registreert, en wijzig waar nodig.

~~Impliciet~~ → Uitdrukkelijk

In praktijk – 13 stappen…

8. KINDEREN

Ontwikkel systemen die de leeftijd van de betrokkene nagaan en die de ouder(s) of voogd(en) om toestemming vragen voor de gegevensverwerking van minderjarige kinderen.

9. DATALEKKEN

Voorzie adequate procedures om persoonlijke datalekken op te sporen, te rapporteren en te onderzoeken.

- ✓ Meldplicht binnen 72 uren na vaststelling
- ✓ Aan DPA
  - Aard van het datalek
  - Categorieën/hoeveelheid betrokkene datasubjecten en databestanden
  - Gevolgen van het datalek
  - Te nemen maatregelen
- ✓ DPA krijgt onderzoeksbevoegdheden
- ✓ *Aan betrokkenen werknemers (HR data)*

In praktijk – 13 stappen…

10. GEGEVENSBESCHERMING DOOR ONTWERP EN GEGEVENSBESCHERMINGSEFFECTBEOORDELING

Maak je vertrouwd met de begrippen "gegevensbescherming door ontwerp" en "gegevensbeschermingseffectbeoordeling" en ga na hoe je deze concepten in de werking van jouw bedrijf of organisatie kan implementeren.

- ✓ Risicoanalyse
- ✓ *"High risk"* HR activiteiten:
  - Rekrutering
  - Screening
  - Evaluatie en beoordeling
  - Ontslag
- ✓ Advies Privacycommissie

- ✓ Privacy door ontwerp en door standaardinstellingen
- ✓ Voorbeelden :
- De verwerking van persoonsgegevens tot een minimum beperken
  - Pseudonimiseren
  - Opt-in i.p.v. opt-out
  - Beveiligingskenmerken

In praktijk – 13 stappen…

11. FUNCTIONARIS VOOR GEGEVENSBESCHERMING

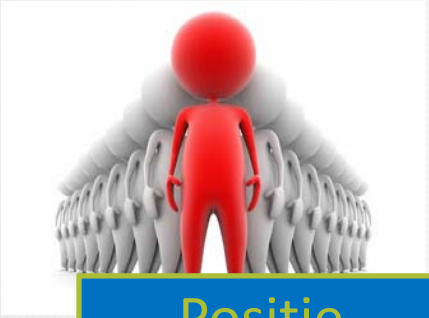
Duid, indien nodig, een functionaris voor gegevensbescherming aan, of iemand die de verantwoordelijkheid draagt voor het naleven van de databeschermingsregels. Beoordeel welke plaats deze inneemt binnen de structuur en het beleid van jouw bedrijf of organisatie.

Verplichte gevallen

Een Functionaris voor Gegevensbescherming moet aangeduid worden wanneer:

- de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan, behalve bij gerechten in de uitoefening van hun rechterlijke taken
- een verwerkingsverantwoordelijke hoofdzakelijk is belast met verwerkingen die regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen;
- de verwerkingsverantwoordelijke hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens zoals strafrechtelijke veroordelingen en strafbare feiten.

Functionaris voor gegevensbescherming



Positie

1. DPO naar behoren en tijdig betrekken bij alle aangelegenheden die verband persoonsgegevens

2. DPO ondersteunen bij zijn taken door hem de nodige toegangen te verschaffen en door hem de benodigde middelen ter beschikking te stellen voor het vervullen van deze taken en het in stand houden van zijn deskundigheid

3. DPO ontvangt geen instructies met betrekking tot de uitvoering van zijn taken

4. DPO wordt niet ontslagen of gestraft voor de uitvoering van zijn taken en brengt rechtstreeks verslag uit aan de hoogste leidinggevende

5. Geen belangenconflict + gehouden tot geheimhouding en vertrouwelijkheid

6. DS kan met DPO contact opnemen voor het uitoefenen van zijn rechten

Functionaris voor gegevensbescherming

Taken

- de verwerkingsverantwoordelijke of de verwerker en de werknemers **informeren en adviseren** over hun verplichtingen uit hoofde van deze verordening en andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen
- **toezien op** naleving van deze verordening, van andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen en van het beleid van de verwerkingsverantwoordelijke of de verwerker
- **advies verstrekken** met betrekking tot de gegevensbeschermingseffect-beoordeling en toezien op de uitvoering daarvan
- met de toezichthoudende autoriteit **samenwerken**

In praktijk – 13 stappen…

12. INTERNATIONAAL

Bepaal onder welke toezichthoudende autoriteit je valt indien jouw bedrijf of organisatie internationaal actief is.

- ✓ Doorzenden binnen EU: adequaat beschermingsniveau
- ✓ Doorzenden van gegevens buiten EU
  - Safe Harbor: ongeldig verklaard
  - Privacyshield: wankel
  - Modelclausules & Binding Corporate Rules: uitdrukkelijk erkend in AVG
- ✓ Goedkeuring DPA vereist

13. BESTAANDE CONTRACTEN

Beoordeel je bestaande contracten, hoofdzakelijk met verwerkers en onderaannemers, en breng tijdig de noodzakelijke veranderingen aan.

Themadossier

aanbeveling over de verwerking van persoonsgegevens door Facebook via cookies, social plug-ins en pixels.

Lees ook onze andere thema's

ALGEMENE VERORDENING GEGEVENS-BESCHERMING ("GDPR") NEW

PRIVACYTHEMA'S
Waar wij dagelijks rond werken

WETGEVING EN NORMEN
Referentieteksten rond gegevensbescherming

BESLISSINGEN
Onze adviezen, machtigingen & aanbevelingen

PUBLICATIES
Publicaties van de Privacycommissie

OVER CBPL
Meer informatie over de Privacycommissie

CONTACTEER ons

MELDING gegevenslek

MACHTIGING aanvragen

AANGIFTE indienen of beheren

Verwante websites

ikbeslis.be

Een specifieke website over jongeren en privacy

anthologieprivacy.be

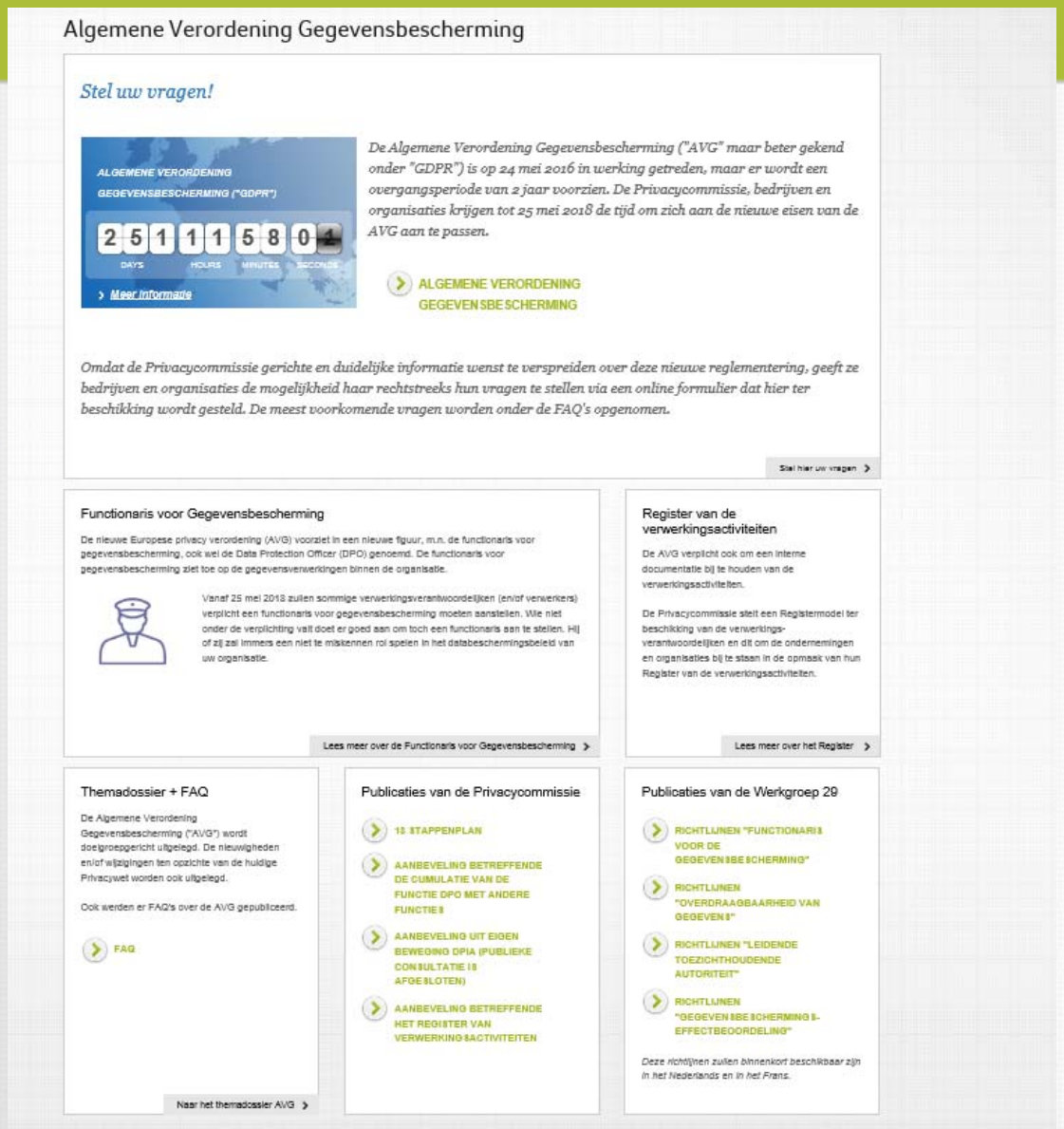
Op deze website vindt u een overzicht van privacygerelateerde artikels.

In de kijker

25 mei 2017: Nog 1 jaar voor de daadwerkelijke toepassing van de Algemene Verordening (AVG) - Privacycommissie: "Wel tanden, geen Pitbull"!

De Algemene Verordening gegevensbescherming, ook gekend als « GDPR », is in werking getreden op 24 mei 2016 maar de daadwerkelijke toepassing is voorzien op 25 mei 2018: nog 1 jaar dus.

Themadossier



- ✓ Themablokken Register en DPO
- ✓ FAQ
- ✓ Publicaties
- ✓ Richtsnoeren Werkgroep 29

Bedankt voor uw aandacht!
www.privacycommision.be