Algemene Verordening Gegevensbescherming (AVG)

General Data Privacy Regulation (GDPR)

Wat betekent dit concreet?

AVG GDPR – Wat betekent dit concreet?

Versie : 1.1

Auteur : Jan Paredis

Vooraleerst …

Dit is een presentatie ten persoonlijke titel. De teksten die ik schrijf representeren mijn eigen mening en stemmen niet altijd overeen met de mensen, bedrijven of organisaties waarmee ik één of andere relatie heb, behalve als dit expliciet vermeld wordt.

Jan Paredis

Opleiding:
TEW – Beleidsinformatie

Ervaring:
CERA (nu KBC), Citibank, IMSHealth/Synavant, Citibank

April 2006 – december 2016: Group Information Security Officer EMEA voor Citibank – Consumer.
Januari 2017 – heden: Chief Information Security Officer VUB

Data Protection Officer (DPO) 'gecertificeerd', samenwerkend met de VUB DPO in

VUB INFORMATIEVEILIGHEID & PRIVACY
INFORMATION SECURITY & PRIVACY

Tot 49

Wat is GDPR?

De GDPR is een verodening waarmee de Europese Commissie de persoonsgegevens van de individuen binnen de Europese Unie (EU) strenger beschermt. De GDPR geldt voor alle landen in de EU en legt ook de regels vast voor het exporteren van persoonsgegevens buiten de EU.

Tegen **25 mei 2018** moeten organisaties **passende technische en organisatorische maatregelen** hebben doorgevoerd **en dat kunnen aantonen**. Verder zijn bedrijven verplicht om deze maatregelen doorlopend te beoordelen en indien nodig bij te stellen. Na 25 mei 2018 kunnen **sancties** worden opgelegd aan diegenen die niet aan de regels voldoen.

Begin op tijd met voorbereidingen zodat u en uw organisatie er op tijd klaar voor zijn. Zorg dat iedereen in uw onderneming bekend is met de nieuwe privacyregels.

Voor wie is de GDPR?

Deze Europese privacywetgeving is er voor alle bedrijven en organisaties die persoonsgegevens vastleggen van klanten, personeel of andere personen uit de EU. Vrijwel alle ondernemers krijgen ermee te maken, ook zelfstandigen en kleine kmo's. Door het versturen van een offerte, factuur of (digitale) nieuwsbrief. Of het bijhouden van afspraken met klanten, contactgegevens van klanten (zoals adres, e-mailadres of telefoonnummers) of personeelsinformatie.

Tip: info@bedrijf.be is geen persoonsgegeven maar een bedrijfsgegeven. Zo is ook het algemene nummer van een bedrijf. U kan dus vrij e-mailen en/of bellen naar een bedrijf (niet naar individuele werknemers van het bedrijf).

Hoe compliant worden?

Besef dat de GDPR een nieuw regelgeving is waar niemand al ervaring mee heeft. Hoe 'streng' gaat de **Gegevensbeschermingsautoriteit** (de nieuwe naam van de Privacycommissie) optreden? Welke interpretaties en verwachtingen gaat deze hebben t.o.v. deelaspecten van de GDPR?

Enkele sleutelelementen:

- **Functionaris voor de gegevensbescherming Data Protection Officer (DPO)**
- **Register (van de verwerkingsactiviteiten)**
- **Privacyverklaring**
- **Data Protection Impact Assessment (DPIA)**
- **Privacy by Design en Privacy by Default**
- **Beveilig je persoonsgebonden data**

DPO – heb je er een nodig? (art 37)

Functionaris gegevensbescherming (DPO)

Aanstelling van een DPO is verplicht wanneer:

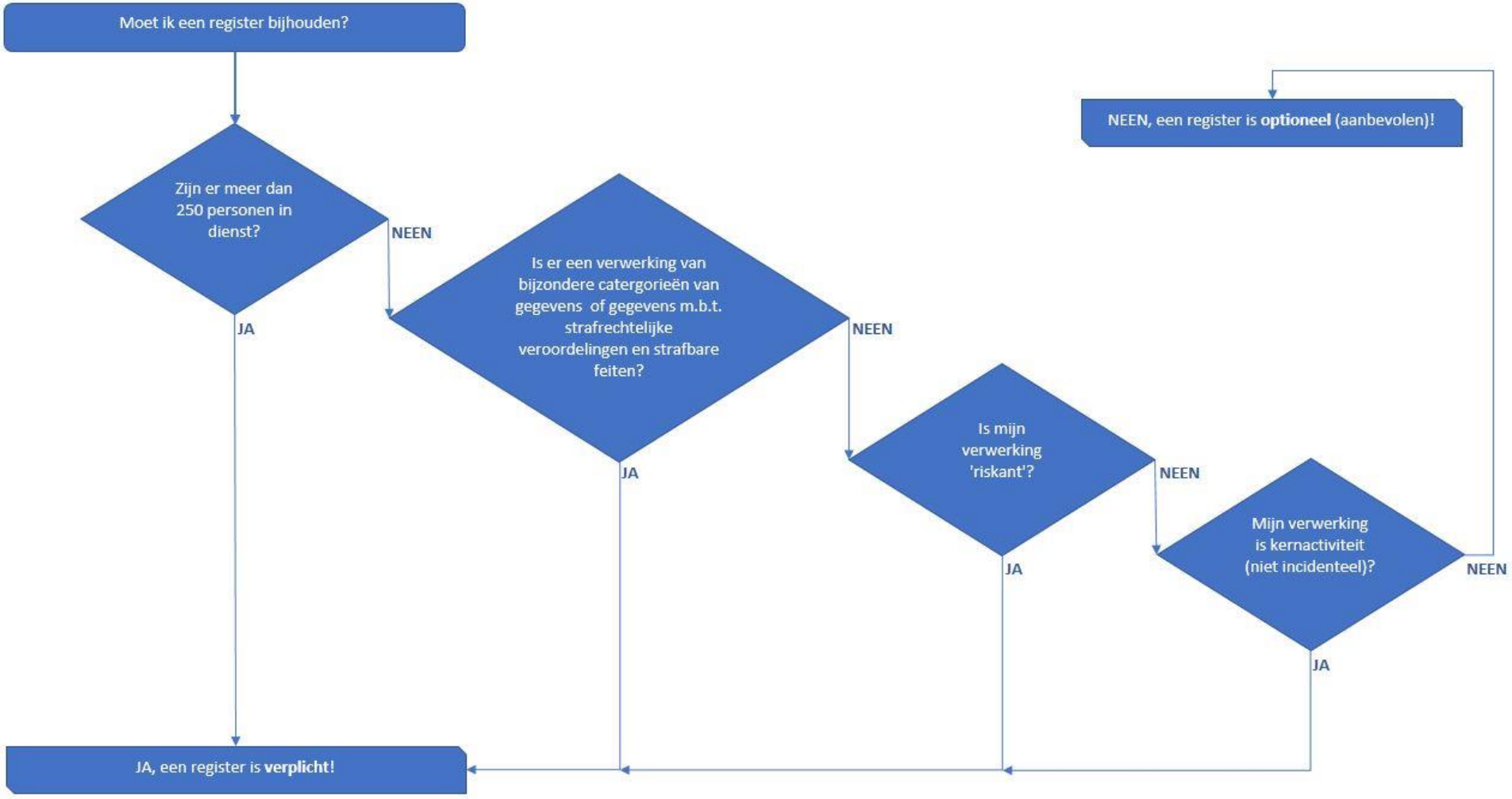
- voor overheidsinstanties/organen;
- het de kernactiviteit van uw bedrijf is om op grote schaal gevoelige persoonsgegevens (zoals gezondheidsgegevens) te verwerken;
- uw organisatie structureel mensen observeert (fysiek of digitaal, bijvoorbeeld via cameraobservatie).

Intern of extern

De positie van de DPO kan vanuit uw organisatie worden ingevuld, maar de functie kan ook door een externe partij worden vervuld.

Aandacht voor naleving van de GDPR is ook van belang voor organisaties die niet verplicht zijn een DPO aan te stellen.

Register – Heb je er een nodig? (art 30)



Register – Inhoud

- Naam en contactgegevens van verwerkingsverantwoordelijke(n) of verwerker (VV & VW);
- Verwerkingsdoeleinden (VV);
- Categorieën van persoonsgegevens en betrokkenen (VV);
- Categorieën van ontvangers (o.a. derde landen of organisaties) (VV);
- Doorgifte van persoonsgegevens aan derde landen en documentatie inzake passende waarborgen (VV & VW);
- Beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist (VV & VW);
- Algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen (VV & VW);
- Categorieën van verwerkingen die worden uitgevoerd (VW).

VV = verwerkingsverantwoordelijke

VW = verwerker

Register – Template privacycommissie

https://www.privacycommission.be/nl/model-voor-een-register-van-de-verwerkingsactiviteiten

	A	D	J	S	V
1	**Register van de verwerkingsactiviteit**				
2	**Verantwoordelijke voor de gegevensverwerking:**				
12	**Functionaris voor de gegevensbescherming:**				
18					
19	**businessproces/verwerking**	**functionele omschrijving verwerking**	**gebruikte gegevens en betrokkenen**	**verwerker**	**gegevensuitwisseling**
20	identificatie van het businessproces *naam, eigenaar proces* *(in de kolom hieronder wordt ifv de leesbaarheid van de elektronische versie van het register, de naam van de verwerking hernomen)*	identificatie en informatie over de verwerking *nummer , functionele omschrijving , finaliteit, verwerkingsgrond, type verwerking en functionele beschrijving*	details over de gegevens die verwerkt worden en de betrokkenen van wie gegevens verwerkt worden *functionele categorie, gevoelige categorie gegevensverwerking, categorie betrokken, classificatieniveau, bewaartermijn, authentieke bron*	identificatie van de verwerker (extern aan organisatie) die betrokken is bij de verwerking *naam, nr gegevensverwerkingscontract*	informatie over eventuele gegevensuitwisseling met derde partijen categorie(ën) gegevens,*categorie(ën) ontvangers, derde land/internationale organisatie, documenten passende waarborgen*
21					

	AB	AD	AI	AL	AQ
1					
2					
12					
18					
19	**technologie**	**risico & beveiligingsmaatregelen**	**rechten betrokkenen**	**status**	**opmerking**
20	beschrijving van de gebruikte technologie, applicaties, software bij de verwerking	informatie over het risico en de beveiligingsmaatregelen van de gegevensverwerking *risico, beschrijving beveiligingsmaatregelen, documentatie beveiligingsmaatregelen, GEB (DPIA)*	verwijzing naar de documenten die de procedures ter respectering van de rechten van de betrokkenen bepalen	informatie over de status van de verwerking: startdatum, einddatum en plaatsvervangende verwerking	noteer eventuele opmerkingen/aandachtspunten mbt de verwerkingsactiviteit
21					
22					

Privacyverklaring (art 13)

GDPR Artikel 13 somt de te verstrekken informatie wanneer persoonsgegevens bij de betrokkene worden verzameld op.

Mensen wiens gegevens je gebruikt moet je proactief informeren over het gebruik van hun persoonsgegevens en hun rechten door jouw organisatie. Dit moet beknopt, transparant, in een duidelijke eenvoudige taal zijn.

Je kan een algemene privacyverklaring centraal plaatsen (bv. op je website) waarnaar je verwijst in je verschillende documenten zoals vrijwilligersnota, lidkaart,... Op de verkorte vermelding meld je wel welke gegevens je voor die actie (bv ledenregistratie) opvraagt en hoe je ze beschermd en bewaard. Met dan een verwijzing naar je algemene privacyverklaring op je website.

Er is geen toestemming nodig van de betrokkenen voor je privacyverklaring.

Privacyverklaring voorbeeld

Hierbij vind je een voorbeeld van privacyverklaring. Je kan niet zomaar deze verklaring knippen en plakken aangezien je verklaring afhankelijk is van je eigen beslissingen rond het verwerken van persoonsgegevens (denk maar aan de keuze uit de wettelijke gronden, bewaartermijn,…)

Je kan dit voorbeeld natuurlijk wel als handleiding gebruiken.

De bruine tekst is facultatief, niet verplicht maar misschien wil je wel dergelijke extra informatie bezorgen aan de personen die je verklaring lezen.

Bron: http://scwitch.be/wp-content/uploads/2018/02/privacy-verklaring-vb-5-feb.pdf

Privacyverklaring vb (2)

…NAAM ORGANISATIE… hecht veel waarde aan de bescherming van uw persoonsgegevens (en dat uw privacy wordt gerespecteerd). In deze privacyverklaring willen we heldere en transparante informatie geven over (welke gegevens we verzamelen) hoe wij omgaan met persoonsgegevens. Wij doen er alles aan om uw privacy te waarborgen en gaan daarom zorgvuldig om met persoonsgegevens.

…NAAM ORGANISATIE… houdt zich in alle gevallen aan de toepasselijke wet- en regelgeving, waaronder de Algemene Verordening Gegevensbescherming. Dit brengt met zich mee dat wij in ieder geval:

- uw persoonsgegevens verwerken in overeenstemming met het doel waarvoor deze zijn verstrekt, deze doelen en type persoonsgegevens zijn beschreven in deze Privacy verklaring;

Bron: http://scwitch.be/wp-content/uploads/2018/02/privacy-verklaring-vb-5-feb.pdf

Privacyverklaring vb (3)

• verwerking van uw persoonsgegevens beperkt is tot enkel die gegevens welke minimaal nodig zijn voor de doeleinden waarvoor ze worden verwerkt;
• vragen om uw uitdrukkelijke toestemming als wij deze nodig hebben voor de verwerking van uw persoonsgegevens;
• passende technische en organisatorische maatregelen hebben genomen zodat de beveiliging van uw persoonsgegevens gewaarborgd is;
• geen persoonsgegevens doorgeven aan andere partijen, tenzij dit nodig is voor uitvoering van de doeleinden waarvoor ze zijn verstrekt;
• op de hoogte zijn van uw rechten omtrent uw persoonsgegevens, u hierop willen wijzen en deze respecteren.

—> facultatief omdat je eigenlijk gewoon weergeeft dat je de wet volgt

Bron: http://scwitch.be/wp-content/uploads/2018/02/privacy-verklaring-vb-5-feb.pdf

Privacyverklaring vb (4)

Als …NAAM ORGANISATIE… zijn wij verantwoordelijk voor de verwerking van uw persoonsgegevens. Indien u na het doornemen van onze privacy verklaring, of in algemenere zin, vragen heeft hierover of contact met ons wenst op te nemen kan dit via onderstaande contactgegevens:

…NAAM ORGNISATIE…
straat nummer
postcode stad
info@naam.be
Telefoon : 02/xxx xxx xxx

Bron: http://scwitch.be/wp-content/uploads/2018/02/privacy-verklaring-vb-5-feb.pdf

Privacyverklaring vb (5)

Waarom verwerken wij persoonsgegevens

Uw persoonsgegevens worden door …NAAM ORGANISATIE… verwerkt ten behoeve van de volgende doeleinden en rechtsgronden :

- om te kunnen deelnemen aan de activiteiten van … NAAM ORGANISATIE…; (uitvoering overeenkomst)
- Het versturen van nieuwsbrieven en uitnodigingen. (toestemming betrokkene)
- Het bekomen van subsidiëring door de overheid (wettelijke verplichting)

(bovenstaande opsomming is een voorbeeld. Jijzelf beslist intern welke wettelijke gronden van toepassing zijn)

Bron: http://scwitch.be/wp-content/uploads/2018/02/privacy-verklaring-vb-5-feb.pdf

Privacyverklaring vb (6)

Voor de bovenstaande doelstellingen kunnen wij de volgende persoonsgegevens van u vragen (en opslagen) (verzamelen) (verwerken) :

- Persoonlijke identiteitsgegevens : naam, voornaam, adres, telefoonnummer, e-mail
- Identiteitsgegevens uitgegeven door overheid : identiteitskaartnummer
- Rijksregisternummer
- Persoonlijke kenmerken : geslacht, geboortedatum, geboorteplaats, nationaliteit
-

(bovenstaande opsomming is een voorbeeld, de oplijsting is afhankelijk van welke gegevens je organisatie gebruikt)

We gebruiken de verzamelde gegevens alleen voor de doeleinden waarvoor we de gegevens hebben verkregen.

Bron: http://scwitch.be/wp-content/uploads/2018/02/privacy-verklaring-vb-5-feb.pdf

Privacyverklaring vb (7)

Verstrekking aan derden

De gegevens die u aan ons geeft kunnen wij aan derde partijen verstrekken indien dit noodzakelijk is voor uitvoering van de hierboven beschreven doeleinden.

Zo maken wij gebruik van een derde partij voor:

- het verzorgen van de internet omgeving (webhosting);
- het verzorgen van IT-infrastructuur (o.a. IT netwerk, …);
- het verzorgen (en verspreiden) van nieuwsbrieven en uitnodigingen.
-

Wij geven nooit persoonsgegevens door aan andere partijen waarmee we geen verwerkersovereenkomst hebben afgesloten.

Bron: http://scwitch.be/wp-content/uploads/2018/02/privacy-verklaring-vb-5-feb.pdf

Privacyverklaring vb (8)

Met deze partijen (verwerkers) maken wij hierin uiteraard de nodige afspraken om de beveiliging van uw persoonsgegevens te waarborgen.
Verder zullen wij de door u verstrekte gegevens niet aan derden doorgeven (andere partijen verstrekken), tenzij dit wettelijk verplicht en toegestaan is. Een voorbeeld hiervan is dat de politie in het kader van een onderzoek (persoons)gegevens bij ons opvraagt. In een dergelijk geval dienen wij medewerking te verlenen en zijn dan ook verplicht deze gegevens af te geven.

Tevens kunnen wij persoonsgegevens delen met derden indien u ons hier (schriftelijk) toestemming voor geeft. U heeft het recht deze toestemming ten allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking voor de intrekking daarvan.

Bron: http://scwitch.be/wp-content/uploads/2018/02/privacy-verklaring-vb-5-feb.pdf

Privacyverklaring vb (9)

Wij verstrekken geen persoonsgegevens aan partijen welke gevestigd zijn buiten de EU.

Minderjarigen

Wij verwerken enkel en alleen persoonsgegevens van minderjarigen (personen jonger dan 16 jaar) indien daarvoor schriftelijke toestemming is gegeven door de ouder of wettelijke vertegenwoordiger.

Bewaartermijn

…NAAM ORGANISATIE… bewaart persoonsgegevens niet langer dan noodzakelijk voor het doel waarvoor deze zijn verstrekt dan wel op grond van de wet is vereist.

(De blauwe tekst is niet voldoende. Je moet expliciet de termijn meedelen! Als algemene regels worden persoonsgegevens maximaal 5 jaar na laatste gebruik bijgehouden, je mag ook omschrijvingen gebruiken zoals: 'De gegevens worden niet langer dan één jaar bewaard').

Bron: http://scwitch.be/wp-content/uploads/2018/02/privacy-verklaring-vb-5-feb.pdf

Privacyverklaring vb (10)

Beveiliging van de gegevens

Wij hebben passende technische en organisatorische maatregelen genomen om persoonsgegevens van u te beschermen tegen onrechtmatige verwerking, zo hebben we bijvoorbeeld de volgende maatregelen genomen;

- Alle personen die namens …NAAM VZW… van uw gegevens kennis kunnen nemen, zijn gehouden aan geheimhouding daarvan.
- We hanteren een gebruikersnaam en wachtwoordbeleid op al onze systemen;
- We pseudonimiseren en zorgen voor de encryptie van persoonsgegevens als daar aanleiding toe is;
- Wij maken back-ups van de persoonsgegevens om deze te kunnen herstellen bij fysieke of technische incidenten;
- We testen en evalueren regelmatig onze maatregelen;
- Onze medewerkers zijn geïnformeerd over het belang van de bescherming van persoonsgegevens.

Bron: http://scwitch.be/wp-content/uploads/2018/02/privacy-verklaring-vb-5-feb.pdf

Privacyverklaring vb (11)

Uw rechten omtrent uw gegevens

U heeft recht op inzage en recht op correctie of verwijdering van de persoonsgegeven welke wij van u ontvangen hebben. Bovenaan dit privacy statement staat hoe je contact met ons kan opnemen. (U kan ons ook contacteren via de contactpagina van onze website …www.NAAM.be…). (om misbruik te voorkomen kunnen wij u daarbij vragen om u adequaat te identificeren). Om uw identiteit te controleren vragen wij u om een kopie van uw identiteitskaart mee te sturen. We raden je sterk aan om daarbij je pasfoto onzichtbaar te maken en erbij te vermelden dat het om een kopie gaat.

Tevens kunt u bezwaar (verzet) maken tegen de verwerking van uw persoonsgegevens (of een deel hiervan) door ons of door één van onze verwerkers. Ook heeft u het recht om de door u verstrekte gegevens door ons te laten overdragen aan uzelf of in opdracht van u direct aan een andere partij. Wij kunnen u vragen om u te legitimeren voordat wij gehoor kunnen geven aan voornoemde verzoeken.

Bron: http://scwitch.be/wp-content/uploads/2018/02/privacy-verklaring-vb-5-feb.pdf

Privacyverklaring vb (12)

Klachten

Mocht u een klacht hebben over de verwerking van uw persoonsgegevens dan vragen wij u hierover direct contact met ons op te nemen.
U heeft altijd het recht een klacht in te dienen bij de Gegevensbeschermingsautoriteit (contact/URL).

Wijziging privacy statement

…NAAM ORGANISATIE… kan zijn privacy statement wijzigen. Van deze wijziging zullen we een aankondiging doen op onze website.
De laatste wijziging gebeurde op …25 oktober 2017…
Oudere versies van ons privacy statement zullen in ons archief worden opgeslagen. Stuur ons een e-mail als u deze wilt raadplegen.

Bron: http://scwitch.be/wp-content/uploads/2018/02/privacy-verklaring-vb-5-feb.pdf

Privacyverklaring vb (13)

voorbeeld beknopte versie

Uw persoonsgegevens worden verwerkt door **(vereniging Gemeente, naamstraat 20 te 9000 Gemeente, info@vereniging.be)**, voor ledenbeheer en organisatie van activiteiten op basis van de contractuele relatie als gevolg van uw inschrijving en om u op de hoogte te houden van onze activiteiten (direct marketing) op basis van ons gerechtvaardigd belang om …(doel of missie vereniging).

Indien u niet wil dat wij uw gegevens verwerken met het oog op direct marketing, volstaat het ons dat mee te delen op **(**info@vereniging.be**)**. Via dat adres kan u ook altijd vragen welke gegevens wij over u verwerken en ze verbeteren of laten wissen, of ze vragen over te dragen. Een meer uitgebreid overzicht van ons beleid op het vlak van verwerking van persoonsgegevens vindt u op **(**www.vereniging.be**)**

Bron: http://scwitch.be/wp-content/uploads/2018/02/privacy-verklaring-vb-5-feb.pdf

Onrechtstreeks verkregen persoonsgegevens (art 14)

Indien men persoonsgegevens niet van de betrokkene zijn verkregen, moet de verwerkingsverantwoordelijke de betrokken informeren.

De te verstrekken informatie is ongeveer gelijk dan wanneer je persoonsgegevens rechtstreeks van de betrokkene hebt verkregen.

Nog 24

Voorbeeld toestemming

Klant creatie – input scherm (* = verplicht veld)

*Naam:_____ *Voornaam:_____

*Straat en nr:_____

*Postcode:_____ *Stad:_____

GSM-nummer:_____ *(zo kunnen we u een SMS sturen met datum/uur levering)*

E-mail:_____ *(zo kunnen we u informatie sturen met datum/uur levering)*

Interesses: □ Sport □ Film □ Boeken □ Reizen

(U wordt dan op de hoogte gehouden van acties die in uw interesse liggen)

□ Ik wil op de hoogte worden gehouden van algemene aanbiedingen.

U kan steeds uw informatie aanpassen. Indien u vragen hebt aangaande de privacy van Uw gegevens, kan u de PB Data Protection Officer (Functionaris voor Gegevensbescherming) contacteren via dpo@pb.be. Een formele privacy klacht kan u indienen bij de Gegevensbeschermingsautoriteit (url.be).

DPIA

Wanneer?

Als verantwoordelijke moet u een **data protection impact assessment** (DPIA) uitvoeren wanneer uw gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert. Dit moet u zelf bepalen. De werkgroep van Europese privacytoezichthouders (WP29) heeft een lijst van 9* criteria opgesteld om u hierbij te helpen.
(WP29 wordt de European Data Protection Board - EDPB)

9 criteria om te toetsen of u een DPIA moet uitvoeren

Als vuistregel kunt u hanteren dat u een DPIA moet uitvoeren als uw verwerking aan 2 of meer van de onderstaande 9 criteria voldoet.

DPIA (2)

1. Beoordelen van mensen op basis van persoonskenmerken
Het gaat hierbij onder meer om profiling en het maken van prognoses, met name op basis van kenmerken als iemands beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen.

Voorbeelden hiervan zijn een bank die de kredietwaardigheid van klanten bepaalt (creditscoring), een bedrijf dat DNA-testen aan consumenten levert om gezondheidsrisico's te testen en een bedrijf dat bezoekers van zijn website volgt en op basis daarvan profielen van deze mensen opstelt.

Bron: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia#in-welke-gevallen-moet-ik-een-dpia-uitvoeren-5879

DPIA (3)

2. Geautomatiseerde beslissingen

Het gaat hierbij om beslissingen die voor de betrokkene rechtsgevolgen of vergelijkbare wezenlijke gevolgen hebben. Zo'n gegevensverwerking kan er bijvoorbeeld toe leiden dat mensen worden uitgesloten of gediscrimineerd.

Gegevensverwerkingen met geringe of geen gevolgen voor mensen vallen niet onder dit criterium. In de aankomende WP29-guidelines over profiling volgt hierover meer uitleg.

Bron: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia#in-welke-gevallen-moet-ik-een-dpia-uitvoeren-5879

DPIA (4)

3. Stelselmatige en grootschalige monitoring

Het gaat hierbij om monitoring van openbaar toegankelijke ruimten, bijvoorbeeld met cameratoezicht. Hierbij kunnen persoonsgegevens worden verzameld zonder dat betrokkenen weten wie hun gegevens verzamelt en wat daar vervolgens mee gebeurt. Bovendien kan het onmogelijk zijn voor mensen om zich in openbare ruimten aan deze gegevensverwerking te onttrekken

Bron: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia#in-welke-gevallen-moet-ik-een-dpia-uitvoeren-5879

DPIA (5)

4. Gevoelige gegevens

Het gaat hierbij om bijzondere categorieën van persoonsgegevens (zie artikel 9 van de GDPR), zoals informatie over iemands politieke voorkeuren. Ook strafrechtelijke gegevens vallen hieronder. Tot slot gaat het hier ook om gegevens die over het algemeen als privacygevoelig worden beschouwd, zoals gegevens over elektronische communicatie, locatiegegevens en financiële gegevens.

Bron: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia#in-welke-gevallen-moet-ik-een-dpia-uitvoeren-5879

DPIA (6)

5. Grootschalige gegevensverwerkingen

De GDPR geeft geen definitie van ‘grootschalige gegevensverwerkingen’. WP29 adviseert om met de volgende criteria te bepalen of hiervan sprake is:

de hoeveelheid mensen van wie gegevens worden verwerkt;

de hoeveelheid gegevens en/of de verscheidenheid aan gegevens die worden verwerkt;

de tijdsduur van de gegevensverwerking;

de geografische reikwijdte van de gegevensverwerking.

Bron: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia#in-welke-gevallen-moet-ik-een-dpia-uitvoeren-5879

DPIA (7)

6. Gekoppelde databases

Het gaat hierbij om gegevensverzamelingen die aan elkaar gekoppeld of met elkaar gecombineerd zijn. Bijvoorbeeld databases die voortkomen uit twee of meer verschillende gegevensverwerkingen met verschillende doelen en/of uitgevoerd door verschillende verantwoordelijken, op een manier die betrokkenen niet redelijkerwijs kunnen verwachten.

Bron: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia#in-welke-gevallen-moet-ik-een-dpia-uitvoeren-5879

DPIA (8)

7. Gegevens over kwetsbare personen

Bij het verwerken van dit type gegevens kan een DPIA nodig zijn omdat er sprake is van een ongelijke machtsverhouding tussen de betrokkene en de verantwoordelijke. Dit heeft als gevolg dat betrokkenen niet in vrijheid toestemming kunnen geven of weigeren voor het verwerken van hun gegevens. Het kan hierbij om bijvoorbeeld werknemers, kinderen en patiënten gaan.

Bron: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia#in-welke-gevallen-moet-ik-een-dpia-uitvoeren-5879

DPIA (9)

8. Gebruik van nieuwe technologieën

De GDPR is er duidelijk over dat een DPIA nodig kan zijn bij het gebruik van een nieuwe technologie. De reden hiervoor is dat dit gebruik gepaard kan gaan met nieuwe manieren om gegevens te verzamelen en gebruiken, met mogelijk grote privacyrisico's.

De persoonlijke en maatschappelijke gevolgen van het gebruik van een nieuwe technologie kunnen zelfs nog onbekend zijn. Een DPIA helpt de verantwoordelijke dan om de risico's te begrijpen en te verhelpen. Sommige 'Internet of Things'-toepassingen bijvoorbeeld kunnen een grote impact hebben op het dagelijks leven en de privacy van mensen, waardoor hierbij een DPIA nodig is.

Bron: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia#in-welke-gevallen-moet-ik-een-dpia-uitvoeren-5879

DPIA (10)

9. Blokkering van een recht, dienst of contract

Het gaat hierbij om gegevensverwerkingen die tot gevolg hebben dat betrokkenen:
een recht niet kunnen uitoefenen of;
een dienst niet kunnen gebruiken of;
een contract niet kunnen afsluiten.

Bijvoorbeeld een bank die persoonsgegevens verwerkt om te bepalen of zij een lening aan iemand willen verstrekken.

Bron: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia#in-welke-gevallen-moet-ik-een-dpia-uitvoeren-5879

DPIA (11)

Verantwoordingsplicht

Let op: deze 9 criteria zijn een hulpmiddelen om in te schatten of u een DPIA moet uitvoeren. Ook als u aan slechts één of geen van deze criteria voldoet, moet u goed kunnen onderbouwen waarom u ervoor kiest om geen DPIA uit te voeren. Dit maakt onderdeel uit van de verantwoordingsplicht.

Bron: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia#in-welke-gevallen-moet-ik-een-dpia-uitvoeren-5879

DPIA (12)

Wanneer hoef ik geen DPIA uit te voeren?

U hoeft geen DPIA uit te voeren wanneer uw gegevensverwerking:

- Waarschijnlijk geen hoog privacy risico oplevert.
- Sterk lijkt op een andere gegevensverwerking waarvoor al een DPIA is uitgevoerd.
- Wordt geregeld door een andere Europese of nationale wet en er bij de totstandkoming van deze wet al een DPIA is uitgevoerd. Tenzij de gegevensbeschermingsautoriteit oordeelt dat er toch een DPIA nodig is.
- Op een lijst staat van verwerkingen waarvoor een DPIA niet verplicht is. De GDPR geeft de gegevensbeschermingsautoriteit de mogelijkheid om zo'n lijst op te stellen, maar dit is niet verplicht.

Bron: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia#in-welke-gevallen-moet-ik-een-dpia-uitvoeren-5879

DPIA (13)

Moet ik alsnog een DPIA uitvoeren voor een bestaande verwerking?
Ja, als er iets verandert aan de verwerking waardoor (na de verandering) een hoog privacy risico oplevert. Bv. nieuwe technologie introduceren of de organisatie/maatschappelijke context verandert.

U hoeft dus niet alsnog een DPIA uit te voeren als een van de volgende 3 situaties van toepassing is:
- uw gegevensverwerking levert waarschijnlijk géén hoog privacy risico op; of
- u heeft voor deze verwerking al eens een voorafgaand onderzoek uitvoeren en de verwerking is in de tussentijd niet veranderd; of
- de risico's van de verwerking zijn niet veranderd.

Het is sowieso aan te raden om periodiek een DPIA uit te voeren. Ook als de gegevensverwerking zelf niet is veranderd. Bijvoorbeeld een keer per 3 jaar.

Bron: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia#in-welke-gevallen-moet-ik-een-dpia-uitvoeren-5879

DPIA (14)

Er zijn verschillende methodes om een DPIA uit te voeren. U kunt er zelf een kiezen, als u maar aan de basisvereisten voldoet zoals die in de AVG staan beschreven.

Voorwaarden DPIA: De DPIA moet in ieder geval het volgende bevatten:

Een systematische beschrijving van de beoogde gegevensverwerkingen en de doeleinden hiervan. Beroept u zich op een gerechtvaardigd belang als grondslag voor de verwerking? Neem dit dan ook op in de beschrijving.

Een beoordeling van de noodzaak en de proportionaliteit van de verwerkingen. Dat houdt in: is het verwerken van persoonsgegevens op deze manier noodzakelijk op uw doel te bereiken? En is de inbreuk op de privacy van de betrokkenen (de mensen van wie u gegevens verwerkt) niet onevenredig in verhouding tot dit doel?

Een beoordeling van de privacy risico's voor de betrokkenen.

De beoogde maatregelen om (1) de risico's aan te pakken (zoals waarborgen en veiligheidsmaatregelen) en (2) aan te tonen dat u aan de GDPR voldoet.

Bron: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/data-protection-impact-assessment-dpia#in-welke-gevallen-moet-ik-een-dpia-uitvoeren-5879

Privacy by Design en Default

Privacy by Design: IT-systemen en applicaties beveiligen de persoonsgegevens standaard op een hoog niveau. Bovendien hoeven de gebruikers van de systemen geen extra handelingen te verrichten om de gegevens te beschermen. Er worden standaard zo min mogelijk gegevens verwerkt.

Privacy by Default: De standaardinstellingen van een product of dienst worden altijd zo privacy vriendelijk mogelijk ingesteld.

Praktisch – Aandachtspunten

Punt 1. Wachtwoorden
Kijk kritisch naar wachtwoorden. Zijn ze voldoende complex? Worden ze regelmatig aangepast? Wordt er een verschillend wachtwoord gebruikt per authenticatie (zeker onderscheid werk-privé)?
Tip: https://www.cnet.com/how-to/how-to-check-the-strength-of-your-passwords/
Tip: gebruik een wachtwoord manager (bv. lastpass, 1password)

Punt 2. Toegangsrechten niet aanpassen
Mensen die bij een bedrijf vertrekken behouden vaak de toegangscodes van de systemen.
Tip: Blokkeer het account onmiddellijk bij iemands vertrek. Wissel de wachtwoorden.

Praktisch – Aandachtspunten (2)

Punt 3. Slechte beveiliging gegevens
Wanneer de gegevens die u beheert op straat belanden, gaat u in de fout.
Tip: Zorg voor duidelijke regels voor hoe met persoonsgegevens veilig om te gaan.
Tip: Versleutel draagbare media (bv. laptop/USB stick)

Punt 4. Gebruik van onveilige software
Datalekken ontstaan vaak via computers waarop onveilige software draait.
Tip: Gebruik enkel software, inclusief 'operating system', dat nog door de leverancier wordt ondersteunt. En heb de laatste (security) patches geïnstalleerd.

Praktisch – Aandachtspunten (3)

Punt 5. Datalekken en hacks aangeven bij politie
Er wordt vaak niet of laat gehandeld na een hack of verlies van een toestel met professionele informatie.
Tip: Sluit de gehackte of verloren toestellen meteen af en verander uw wachtwoorden. Meld het datalek binnen 72u na ontdekking bij de Gegevensbeschermingsautoriteit.

Punt 6. Iedereen mailen
Vandaag spammen de meesten er op los. Ze mailen naar mensen die zich ooit op een wedstrijd inschreven, kopen een paar duizend e-mailadressen of voegen elke mailadres dat ze vinden aan hun mailinglist toe.
Tip: U mag enkel de mensen mailen die eerder hun toestemming gaven om uw mailings te ontvangen

Praktisch – Aandachtspunten (3)

Punt 7. Adressenbestand kopen

De meest gemakkelijke manier om uw doelpubliek in een bepaalde sector te vinden? Adressenbestanden kopen.

Is de koper verantwoordelijke voor de wettelijkheid van het bestand (bv. hebben betrokkenen hun toestemming gegeven)? Open voor debat.

Tip: Als u een bestand koopt, neem in het koopcontract op dat de verkoper verantwoordelijk is voor de wettelijkheid van het bestand. Vergeet niet dat u verplicht bent de in het bestand opgenomen betrokkenen een kennisgeving te sturen met een opt-out mogelijkheid.

Praktisch – Aandachtspunten (4)

Punt 8: Bestaande contracten

Ga ook na of alle bestaande contracten in orde zijn. Breng tijdig waar nodig de noodzakelijke veranderingen aan. Want bij bestaande contracten met onderaannemers of in het geval van outsourcing moet nagegaan worden of de veiligheidsmaatregelen nog steeds toereikend zijn.

Als verwerkingsverantwoordelijke blijft u verantwoordelijk!

Praktisch – Bruikbare URL's

- De nieuwe privacywet van A tot Z: https://www.youtube.com/watch?v=-9KkkzAwQd8

- Tips om safe op het web te surfen (bv. herken phishing e-mail): https://www.safeonweb.be/

- Centrum voor Cybersecurity Belgium (o.a. Cyber Security kit): https://www.ccb.belgium.be/nl

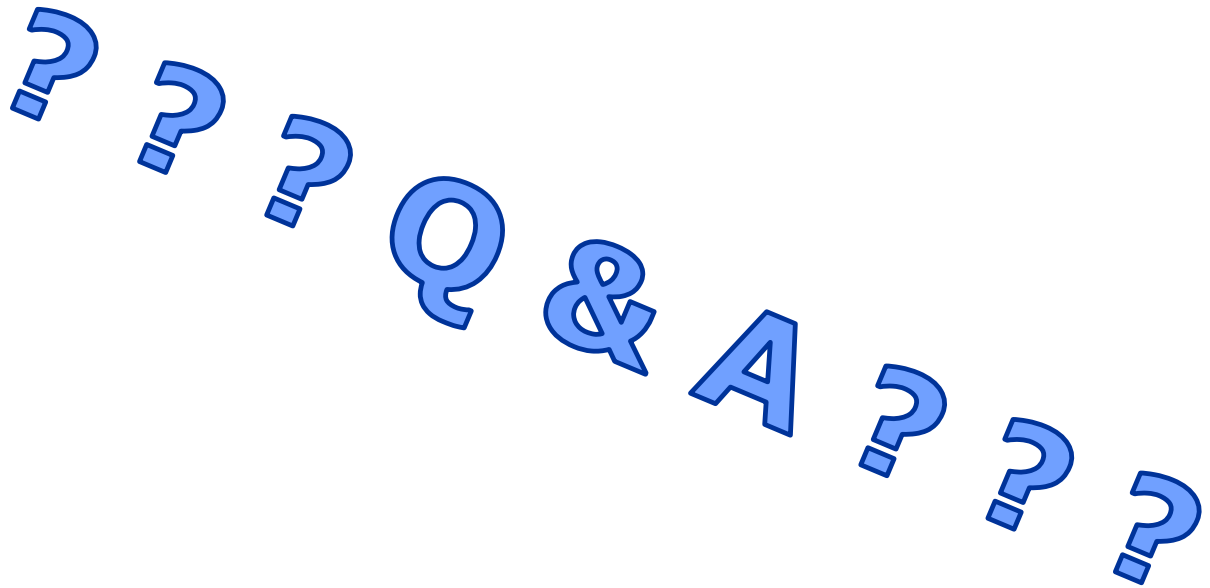
- Cyber Security Coalition: https://www.cybersecuritycoalition.be/

- DPIA door de "Commission Nationale de l'Informatique et des Libertés » (Frankrijk): https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment
  (onder voorbehoud)

Praktisch – Bronnen

- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679
- https://digitaleversnelling.be/
- http://legaldirect.be/
- https://www.privacycommission.be/
- https://www.mt.nl/http://scwitch.be/
- https://autoriteitpersoonsgegevens.nl/
- https://cobofisk.be/nieuwe-privacywetgeving-avg/
- https://www.datalink.be/digitaal-werken/gdpr-voor-kmo/
- https://www.kvk.nl/advies-en-informatie/avg/

IVP Awareness – Vragen



Geen garantie op antwoorden!