VBO
Verbond van Belgische Ondernemingen

CYBER SECURITY COALITION.be

DATA PROTECTION

De gevolgen van de nieuwe algemene verordening gegevensbescherming voor ondernemingen toegelicht

- Nieuwe regelgeving afdwingbaar vanaf **25 mei 2018**
- Van **toepassing** op alle ondernemingen in de EU
- Strenge **boetes** bij inbreuk

WAAROM DEZE BROCHURE?

Onze wereld is steeds meer met elkaar geïnterconnecteerd. Naarmate persoonsgegevens almaar sneller en in grotere getale circuleren, wordt ook de bescherming van die gegevens en van de privacy van de betrokken personen een centrale bekommernis.

Een nieuwe Europese Verordening stelt dan ook strengere eisen waaraan ondernemingen – iedere organisatie die persoonsgegevens verwerkt – moeten voldoen.
De General Data Protection Regulation of 'GDPR', zoals de Verordening afgekort heet, is erg complex. Met deze brochure als leidraad wil het VBO duidelijk maken waar het bij bescherming van persoonsgegevens om gaat en hoe u tewerk moet gaan.

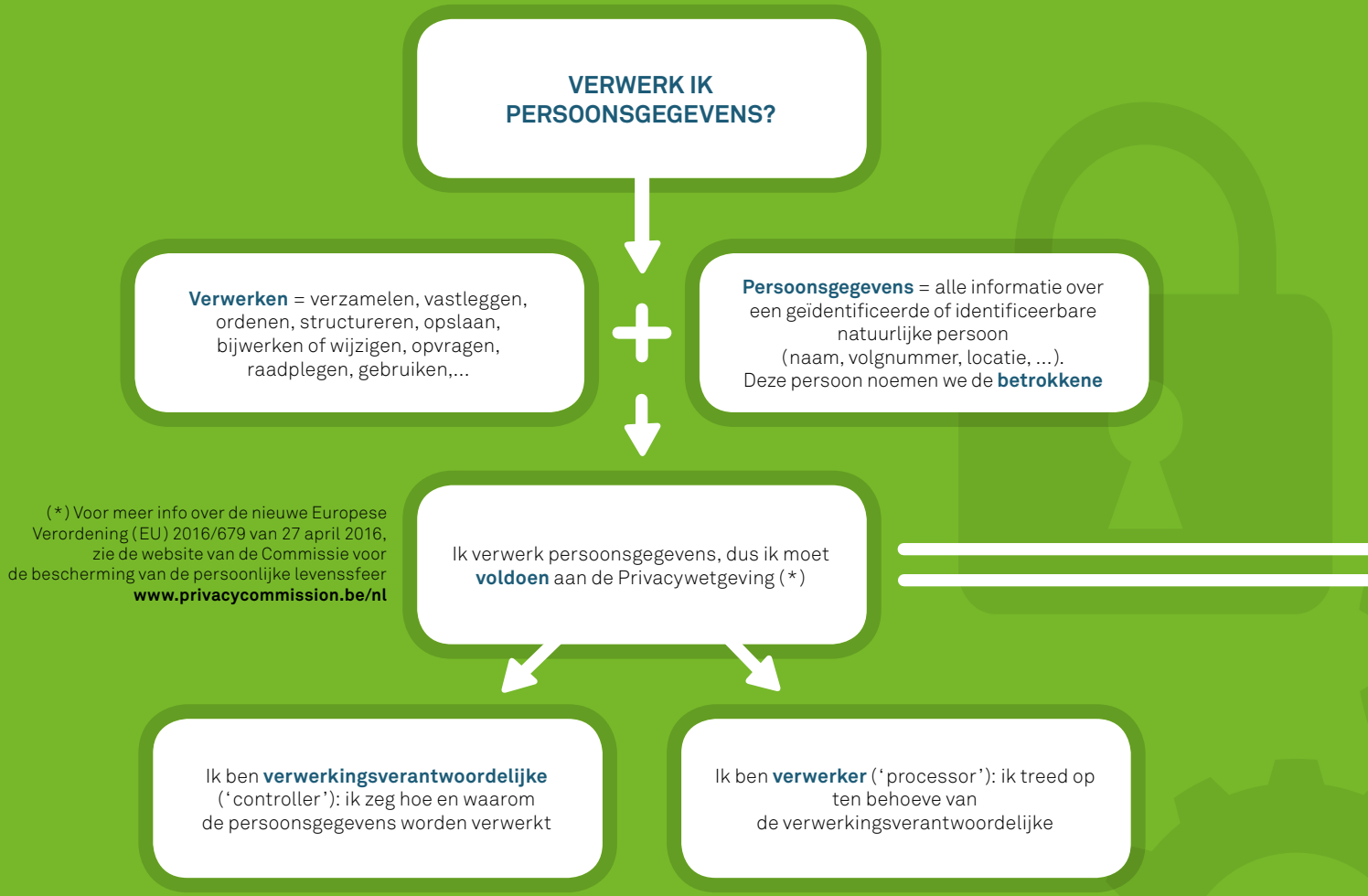
GDPR IS EEN ZAAK VAN IEDEREEN!

Op 25 mei wordt GDPR van kracht! Wat betekent dit concreet? Elke onderneming of organisatie die persoonsgegevens (eigen personeel, personeel van leveranciers, klanten, prospecten, enz.) bijhoudt of gebruikt, zal moeten kunnen aantonen dat ze dit doet met het respect van de regels van GDPR.

'Compliance' met de GDPR is niet iets dat je van vandaag op morgen voor elkaar krijgt. Het vraagt bovendien niet alleen een grondige kennis van GDPR, maar ook van je onderneming of organisatie.

De Cyber Security Coalition wil bedrijven en organisaties op de goede weg zetten door hen een aantal tools aan te reiken. Wie deze brochure heeft gelezen, bezit meteen een goede basiskennis van GDPR. Daarnaast biedt de Coalition ook een 'GDPR checkUp' aan die een onderneming of organisatie toelaat om zelf op een eenvoudige manier te evalueren welke stappen ze moet nemen om tegen 25 mei 2018 in orde te zijn.

De 'GDPR checkUp' vind je via **www.cybersecuritycoalition.be.**


VERWERK IK PERSOONSGEGEVENS?
Verwerken = verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken,...
Persoonsgegevens = alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (naam, volgnummer, locatie, ...). Deze persoon noemen we de **betrokkene**
(*) Voor meer info over de nieuwe Europese Verordening (EU) 2016/679 van 27 april 2016, zie de website van de Commissie voor de bescherming van de persoonlijke levenssfeer **www.privacycommission.be/nl**
Ik verwerk persoonsgegevens, dus ik moet **voldoen** aan de Privacywetgeving (*)
Ik ben **verwerkingsverantwoordelijke** ('controller'): ik zeg hoe en waarom de persoonsgegevens worden verwerkt
Ik ben **verwerker** ('processor'): ik treed op ten behoeve van de verwerkingsverantwoordelijke

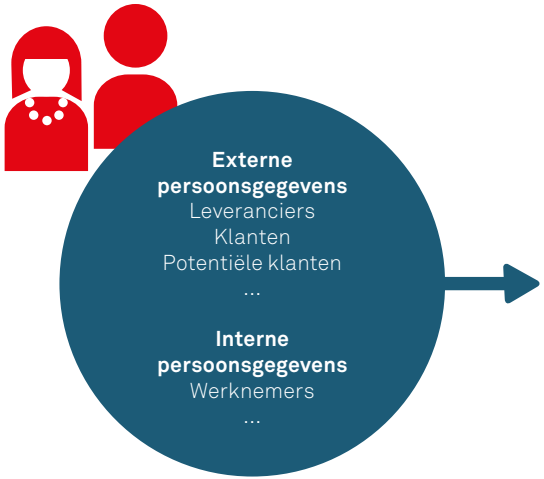
OM TE **VOLDOEN** MOET IK ERVOOR ZORGEN DAT DE PERSOONSGEGEVENS

- verwerkt worden op een **rechtmatige**, **eerlijke wijze** en moet het duidelijk zijn hoe de informatie precies zal gebruikt worden
- enkel verzameld worden voor **welbepaalde**, **uitdrukkelijk omschreven en gerechtvaardigde doeleinden**
- relevant en **beperkt zijn** tot de beoogde doeleinden van de verwerking
- accuraat en **up-to-date zijn**
- **niet langer worden bewaard dan noodzakelijk** voor de beoogde doeleinden van de verwerking
- enkel verwerkt worden op een manier die de **veiligheid van de persoonsgegevens** garandeert

DE **VERANTWOORDINGSPLICHT** VERPLICHT MIJ OM **AAN TE TONEN** DAT

- ik een **data-register** creëer voor alle verwerkingsactiviteiten van persoonsgegevens (inventaris)
- ik er mij van verzeker dat er enkel een **minimum** aan persoonsgegevens, dat noodzakelijk is voor het bereiken van het verwerkingsdoel, wordt verwerkt
- ik een **privacy notice** opstel, i.e. een verklaring die beschrijft hoe mijn onderneming de persoonsgegevens verzamelt, gebruikt, bewaart, ...
- ik een **interne policy** ontwikkel voor het informeren en het trainen van mijn medewerkers
- ik een verantwoordelijke medewerker aanduid voor de gegevensbescherming
- waar nodig, ik een **gegevensbeschermings-impactanalyse** uitvoer. Deze analyse biedt me de mogelijkheid om de meest doeltreffende wijze voor gegevensbescherming te vinden, de risico's te beperken en om de bescherming van deze gegevens te garanderen
- ik voorzie in een implementatie van **efficiënte (beveiligings)procedures** om zeker te zijn dat de privacywetgeving wordt gerespecteerd

WANNEER MAG IK PERSOONSGEGEVENS VERWERKEN?



OFWEL MET TOESTEMMING VAN DE BETROKKENE

OFWEL WANNEER HET NOODZAKELIJK IS

voor het **uitvoeren van een overeenkomst** (bv. verwerken van het adres van iemand die online heeft besteld en waar geleverd moet worden, of verwerken van kredietkaartgegevens om betaling te bekomen, ...)

om te voldoen aan een **wettelijke verplichting** (bv. werkgevers moeten gegevens over werknemers doorgeven aan de sociale zekerheid, financiële instellingen moeten verdachte transacties aangeven, ...)

om de **vitale belangen** van een betrokkene te beschermen

voor het uitvoeren van een taak van **algemeen belang**

voor de behartiging van een **gerechtvaardigd belang** (bv. een onderneming in de nucleaire sector heeft een gerechtvaardigd belang om enkele specifieke persoonsgegevens te verwerken van haar personeel ten einde de veiligheid en gezondheid van dat personeel te kunnen garanderen)

Toestemming vereist een **duidelijke bevestigende handeling**. Stilzwijgen, vooraf aangetikte velden of inactiviteit vormen geen toestemming!
De toestemming moet controleerbaar zijn. Dit betekent dat men moet bijhouden hoe en wanneer de toestemming werd gegeven.
De betrokkene heeft te allen tijde het recht om zijn toestemming **in te trekken**. Het intrekken van deze toestemming moet even eenvoudig zijn als het geven ervan.

PERSOONSGEGEVENS VAN KINDEREN

De General Data Protection Regulation (GDPR) bevat nieuwe strengere regelgeving om de bescherming van persoonsgegevens van kinderen te verbeteren

WAT MET DE REEDS VROEGER VERKREGEN TOESTEMMING?

Er zal geen nieuwe toestemming nodig zijn als de reeds verkregen toestemming voldoet aan de nieuwe vereisten. De systemen moeten wel nagekeken worden om er zeker van te zijn dat de in het verleden verkregen toestemming voldoet aan de nieuwe regelgeving

- Zorg ervoor dat de betrokkene duidelijk ingelicht wordt over de verwerking waarvoor hij toestemming geeft
- Zorg ervoor dat het toestemmingsmechanisme in een werkelijke vrijwillige keuze voorziet en van nature een 'opt-in' situatie is
- Zorg voor een mechanisme waardoor de betrokkene zijn toestemming eenvoudig kan intrekken
- Zorg ervoor dat je je niet baseert op stilzwijgen of inactiviteit om toestemming te bekomen

WAT KAN EEN BETROKKENE VAN ME VRAGEN?

RECHT OM GEÏNFORMEERD TE WORDEN

Ik moet in alle transparantie informatie verstrekken aan de betrokkene over hoe en welke persoonsgegevens ik verwerk (Privacy notice)

Welke informatie ik moet verstrekken, hangt af van het feit of de persoonsgegevens rechtstreeks of onrechtstreeks worden verzameld bij de betrokkene

Deze informatie moet worden verstrekt op het ogenblik dat de persoonsgegevens worden verzameld (rechtstreeks) of binnen een redelijke termijn (onrechtstreeks)

RECHT OP OVERDRAAGBAARHEID VAN GEGEVENS

De betrokkene heeft het recht om de persoonsgegevens die hij heeft verstrekt te laten overdragen naar een andere verwerker

Enkel de gegevens die de betrokkene zelf heeft verstrekt (op basis van toestemming of overeenkomst) moeten worden overgedragen

Ik moet deze gegevens overdragen in een gestructureerde, gangbare en leesbare vorm

Ik moet dit gratis doen en binnen de tijdspanne van één maand (verlengbaar met twee maanden)

RECHT OP VERWIJDERING

De betrokkene kan mij vragen om 'te worden vergeten' en te worden verwijderd uit mijn bestanden (met wettelijke uitzonderingen)

De betrokkene heeft dit recht in specifieke gevallen wanneer de verwerking van persoonsgegevens hem schade berokkent

Er zijn speciale omstandigheden voorzien waarbij ik de vraag tot verwijderen kan weigeren

RECHT OP CORRECTIE

Ik moet de persoonsgegevens corrigeren wanneer deze onjuist of onvolledig zijn

Ik moet derden informeren als ik de te corrigeren persoonsgegevens aan hen heb bezorgd

Ik moet de betrokkene meedelen aan welke derden ik de gegevens heb bezorgd

Ik moet binnen de maand reageren (verlengbaar met twee maanden)

GEAUTOMATISEERDE BESLUITVORMING EN PROFILING

Alle betrokkenen hebben het recht om niet te worden onderworpen aan een volledig geautomatiseerde besluitvorming

In het geval van geautomatiseerde besluitvorming moet ik ervoor zorgen dat de betrokkene de mogelijkheid heeft om (1) menselijke tussenkomst te bekomen; (2) zijn standpunt te kunnen bijbrengen en (3) uitleg te krijgen omtrent de besluitvorming en dit kan betwisten

Het recht geldt niet wanneer de besluitvorming (1) nodig is om een overeenkomst aan te gaan of uit te voeren; (2) wettelijk is toegestaan; (3) gebaseerd is op uitdrukkelijke toestemming

RECHT VAN INZAGE

De betrokkene heeft het recht om te weten of zijn persoonsgegevens worden verwerkt of niet

De verantwoordelijke moet gratis een kopie verstrekken van de verwerkte persoonsgegevens en dit binnen de maand (verlengbaar met twee maanden)

RECHT VAN VERZET

De betrokkene kan zich verzetten tegen

01 - direct marketing: wanneer ik een verzet ontvang, moet ik onmiddellijk stoppen met de verwerking. Hierop zijn geen uitzonderingen

02 - verwerking o.b.v. gerechtvaardigde gronden: wanneer ik een verzet ontvang, kan ik enkel om bepaalde wettelijke redenen nog verder verwerken

03 - verwerking voor **wetenschappelijk of historisch onderzoek** in bepaalde gevallen

Ik moet de betrokkene bij de eerste communicatie informeren van zijn recht op verzet en het uitdrukkelijk vermelden in mijn privacy notice

WAT ZIJN MIJN VERPLICHTINGEN ALS VERANTWOORDELIJKE EN/OF VERWERKER?

Telkens ik een persoonsgegeven verwerk, zal ik dit doen als een verwerkingsverantwoordelijke of als een verwerker. De vorige wetgeving legde enkel verplichtingen op t.a.v. de verantwoordelijke, terwijl er nu ook verplichtingen worden opgelegd aan de verwerker

ALS VERANTWOORDELIJKE MOET IK

- al mijn activiteiten aangaande verwerking van persoonsgegevens nakijken en er controleerbare documentatie van bijhouden
- mij ervan verzekeren dat ik gepaste technische en organisatorische maatregelen heb getroffen om de nodige veiligheid van persoonsgegevens te garanderen
- mij ervan verzekeren dat ik de genomen maatregelen kan aantonen met documentatie en samenwerk met de Privacy-commissie indien nodig
- mij ervan verzekeren dat ik de gepaste processen en projectbrieven heb om bij inbreuk i.v.m. persoonsgegevens (data breach) deze snel te kunnen opmerken, identificeren en aangifte te kunnen doen aan de Privacy-commissie

ALS VERWERKER MOET IK

- mijn bestaande overeenkomsten m.b.t. verwerking van persoonsgegevens nakijken en zorgen voor de noodzakelijke veiligheid en vertrouwelijkheid van de gegevens die ik verwerk
- enkel gegevens op basis van instructies van de verantwoordelijke verwerken
- mij ervan verzekeren dat ik de gepaste processen en projectbrieven heb om bij inbreuk i.v.m. persoonsgegevens (data breach) deze snel te kunnen opmerken, identificeren en aangifte te kunnen doen aan de betrokken verantwoordelijke
- weten dat ik enkel een sub-verwerker mag aanstellen mits akkoord van de verantwoordelijke

WAT ALS IK GEGEVENS DOORGEEF BUITEN DE EU?

WAT IN GEVAL VAN EEN DATA BREACH?

Data Breach betekent een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot persoonsgegevens

Ik moet de Privacy-commissie **verwittigen** van de inbreuk wanneer deze vermoedelijk een risico vormt voor de rechten en vrijheden van personen en dit binnen de 72 uur nadat ik kennis heb genomen van de inbreuk

Wanneer de inbreuk een **hoog risico** zou kunnen vormen voor de rechten en vrijheden van de personen, dan moeten deze personen zelf ook verwittigd worden van de inbreuk

- Zorg ervoor dat jouw medewerkers en personeel weten wat een inbreuk of data breach precies inhoudt
- Duid iemand aan die verantwoordelijk is voor het controleren en het rapporteren van de inbreuk (en)
- Zet een degelijk detectiesysteem op poten
- Bereid een template voor om inbreuken te melden

VERANTWOORDELIJKE PERSOON & DATA PROTECTION OFFICER

HET VBO RAADT ALLE ONDERNEMINGEN AAN OM EEN VERANTWOORDELIJKE PERSOON VOOR DE GEGEVENSBESCHERMING AAN TE DUIDEN

Wanneer de kerntaken van uw onderneming bestaan uit op grote schaal systematisch personen te monitoren of speciale categorieën van gegevens te verwerken, dan bent u **verplicht** een Data Protection Officer (DPO) aan te stellen

DE TAKEN VAN DE DATA PROTECTION OFFICER

De onderneming en haar medewerkers informeren en adviseren omtrent hun verplichtingen om te voldoen aan de regels van de GDPR en andere gegevensbeschermingswetten

Het monitoren van het al dan niet voldoen aan de regels van de GDPR

Het contactpunt zijn in verband met gegevensbescherming

De taak van de DPO **kan toegewezen worden aan een bestaande medewerker** zolang de professionele taken van de medewerker compatibel zijn met deze van de DPO en dit niet leidt tot belangenconflicten

De taak van DPO **kan extern uitbesteed worden**

COLOFON

Redactie
Nathalie Ragheno

Verantwoordelijke uitgever
VBO VZW
Stefan Maes
Ravensteinstraat 4
B - 1000 Brussel
www.vbo.be

Opmaak en ontwerp
manythink

Druk
Graphius

Wettelijk depot
D/0140/2016/15

Cette brochure
est aussi disponible
en français

7 SLEUTELAANBEVELINGEN

1. Hou een inventaris bij van alle verwerkingen van persoonsgegevens, samen met de doelstelling die ze beogen
2. Behandel de geregistreerde gegevens op rechtmatige en transparante wijze
3. Registreer enkel de noodzakelijke data en houd ze niet langer bij dan nodig
4. Tref passende veiligheidsmaatregelen om de gegevens in kwestie te beschermen
5. Informeer duidelijk de personen van wie gegevens worden bijgehouden
6. Werk een intern gegevensbeschermings- en privacybeleid uit
7. Duid iemand aan als verantwoordelijke voor gegevensbescherming en privacy

CENTRE FOR CYBER SECURITY BELGIUM

BNP PARIBAS FORTIS

ING

KBC

proximus

SWIFT

FEB
Fédération des Entreprises de Belgique

Ravensteinstraat 4 - 1000 Brussel
T: + 32 2 515 08 11
info@vbo-feb.be
www.vbo.be

Facebook VBO-FEB
Twitter @VBOFEB
LinkedIn VBO-FEB