GDPR - AVG - PRIVACY vs05.05.18

U heeft er ongetwijfeld al van gehoord, de General Data Protection Regulation. Europese wetgeving die misbruik van persoonlijke gegevens aan banden wil leggen en die op 25/05/18 in werking treedt.

Het gaat over bescherming van **persoonsgegevens** van **natuurlijke personen** (dus privé personen, geen vennootschappen) dewelke **Identificeerbaar** zijn (anonieme data zijn dus geen probleem)

Daarenboven zijn er bijzondere categoriën van persoonsgegevens die een speciale bescherming genieten wegens hun gevoelige aard (en waarvoor je dus expliciete toestemming van betrokkene moet hebben om deze te verwerken) , zoals oa. ras, politieke of levensbeschouweijke overtuiging synsicaal lidmaatschap, genetische of biometrische informatie of seksuele geaardheid.

Wat er wordt er nu concreet van u verwacht ? Dat u zich begint voor te bereiden.

Om u hierin bij te staan hebben wij voor u een stappenpplan uitgewerkt. Dit plan is vanzelfpsrekend geen volledig sluitend dossier maar een leidraad. Onze dossierbeheerders staan u graag bij in de vervollediging ervan.

Praktisch willen wij u alvast adviseren een map aan te leggen voor uw GDPR compliance. Verzamel hierin al uw voorbereidingswerk & verantwoordings stukken. Zo heeft u in een worst case scenario, bewijs van aanpak.

Tot slot nog dit, vanaf 25/05 houdt u best ineens bij het design van nieuwe diensten pf producten rekening met de nieuwe privacy wetgeving. Het principe van “privacy by default” wordt de standaard. U moet er maw voor zorgen dat ieder nieuw product, dienst of procedure in uw bedrijf als standaardwaarde de meest beschermde instelling heeft.

Voor meer info kan u terecht op ons kantoor. Succes !

Patrick Helsen

Checlist Algemene verordening gegevensbescherming, beter bekend als "GDPR" vs 05.05.2018

Uw organisatie moet vanaf 25 mei 2018 in orde te zijn met de AVG[1]- regels. U kan veel informatie over dit onderwerp vinden op de website van de Privacycommissie: https://www.privacycommission.be.

Om u te helpen op een gestructureerde manier te werk te gaan werd een controlelijst opgesteld.

De antwoorden op deze vragen vormen de basis voor de eventuele verdere stappen die u nog dient te nemen. Bij het doorlopen van deze lijst moet men steeds voor ogen houden dat het gaat om de verzameling/bewerking/bewaring van **persoonsgegevens[2]** van **natuurlijke personen** en dit in de contekst van de uitoefening van uw beroep.

[2] **Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;**

12 STAPPEN

- **Stap 1- Maak een overzicht van de persoonsgegevens die u heeft, bewerkt en de wijze waarop u ze bewaart.**
- **Stap 2 - De rechtmatige grondslag voor het verwerken van persoonsgegevens.**
- **Stap 3 - Pas op voor gevoelige persoonsgegevens!**
- **Stap 4 - Vraagt u op een correcte manier toestemming?**
- **Stap 5 - Garandeert u de rechten van de betrokkenen?**
- **Stap 6 - Computert u veilig ?**
- **Stap 7 - Heeft u een Data Protection Officer (DPO) nodig?**
- **Stap 8 - Moet u een Data Protection Impact Assessment (DPIA) uitvoeren?**
- **Stap 9 - Stel een register van de verwerkingsactiviteiten op**
- **Stap 10 - Maak een privacybeleid aan**
- **Stap 11- Relatie met verwerkers**
- **Stap 12 - Wat te doen bij een data-lek?**

Stap 1 – Maak een overzicht van de persoonsgegevens die u heeft, bewerkt en de wijze waarop u ze bewaart

Het opmaken van een soort 'data-inventaris' is een eerste zeer belangrijke stap in uw voorbereiding. U dient in kaart te brengen welke persoonsgegevens u binnen uw beroepsactiviteiten allemaal verwerkt[3].

Het is daarbij aanbevolen dat u deze oefening maakt met bijvoorbeeld een excelbestand of een andere vorm van databestand. Dit bestand zal dan ook de basis vormen voor het gegevensbewerkingregister (stap 9).

VAN WIE HOUDT U PERSOONSGEGEVENS BIJ ?

Hieronder vindt u alvast een aantal categorieën van personen waarvan u mogelijks de persoonsgegevens verwerkt. Let op : dit is geen exclusieve lijst. Misschien verwerkt u er ook nog andere.

- ☐ Klanten
- ☐ Leveranciers
- ☐ Personeel
- ☐ Prospecten
- ☐ Andere: voorbeeld uw bedrijf publiceert een nieuwsbrief voor de klanten maar eenieder die dit wil kan zich inschrijven . …..
- ☐ Bezoekers op uw website

WELKE GEGEVENS ?

Welke categorieën van gegevens betreffende natuurlijke personen verwerkt u?

- ☐ Identiteitsgegevens (naam, adres, telefoonnummer, ondernemingsnummer…)
- ☐ Facturatiegegevens
- ☐ Gevoelige gegevens (gezondheid, foto, lidmaatschap vakbond of politieke partij, kinderen…)
- ☐ Andere: voorbeeld: IP-adressen, cookies, nummerplaten voertuigen, hobbies, verzekeringsgegevens ….

[3] Verwerken = zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op enigerlei andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, evenals het afschermen, uitwissen of vernietigen van persoonsgegevens.

BRON

Waar komen deze persoonsgegevens vandaan?

☐van de betrokken personen zelf

☐Via derden bv via klanten (gegevens over hun leveranciers en klanten),

☐publieke databanken zoals KBO, Nationale Bank van België,

☐Privé- databanken zoals Companyweb, Graydon……..

OPSLAG/TOEGANG/BEWARING ?

Waar slaat u deze persoonsgegevens op? In welke databank(en) en waar bevind(t)(en) die zich? (zie ook de data checklist achteraan in deze bundel)

☐Server op kantoor

☐Server bij een gespecialiseerde provider

☐Cloud in eigen beheer

☐Cloud bij een provider (vb Google, Microsoft, telecombedrijf…)

☐Archief – papier

….

Hoelang houdt u de gegevens bij?

Noteer hier de bewaringstermijnen die bij u van toepassing zijn

Voorbeelden :

- de boekhoudwetgeving vereist dat deze 7 jaar worden bijgehouden.

- Anti-witwas wetgeving vereist dat de in deze contekst verzamelde gegevens bewaard worden gedurende 10 jaar na de stopzetting van de zakelijke relatie

Opgelet: De persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk voor de beoogde doeleinden van de verwerking. De bewaringstermijn van de persoonsgegevens dient dus zorgvuldig te worden nagedacht zodat ze eventueel verantwoord kan worden.

Wie heeft er allemaal toegang tot deze databanken ? Welke functies hebben deze personen? Is de toegang noodzakelijk ?

Maak een tabel/organigram met de verschillende taken van iedereen en bekijk tot welke persoonsgegevens ze eigenlijk toegang moeten hebben om hun taken te kunnen uitvoeren.

Is de toegang beveiligd?

Neem de nodige maatregelen om de toegang tot de persoonsgegevens te beveiligen. Dit kan een digitale beveiliging zijn (login, paswoord), maar evenzeer een slot op de kast waar bepaalde documenten worden bewaard. Maak een overzicht van de verschillende beveiligingen die toegepast worden op kantoor.

Worden deze persoonsgegevens gedeeld met of overgedragen aan derden. Binnen of buiten de EU (cloud ? waar bevindt deze zich ?)

De persoonsgegevens worden gedeeld met:

- Sociaal secretariaat (eigen personeel)
- Fiscale administratie (BTW-aaangiftes voor de klanten, BTW-listings, fiscale fiches …
- Leveranciers ?
- Banken ?

Stap 2 – De rechtmatige grondslag voor het verwerken van persoonsgegevens

U mag enkel persoonsgegevens verzamelen en verwerken wanneer daarvoor één van de grondslagen zoals voorzien door art. 6 AVG, bestaat.

Waarom is het nu zo belangrijk om de grondslag van de verwerking te bepalen?

Afhankelijk van de grondslag kunnen de rechten van de betrokkene variëren. Zo beschikt de betrokkene bv. over meer rechten om de verwijdering van zijn gegevens te vragen indien de persoonsgegevens werden verwerkt op basis van zijn/haar toestemming (zie stap 4).

De rechtmatige grondslag dient ook verduidelijkt te worden in een Privacybeleid (zie stap 10).

Waarom houdt u deze persoonsgegevens bij?

☐ in uitvoering van een overeenkomst /contract met uw klant

☐ in het kader van het personeelsbeheer

☐ wettelijke verplichtingen door uw beroepscategorie opgelegd bv Anti witwas wetgeving, BTW-listing …

☐ in het kader van het beheer van relaties met klanten, leveranciers en andere derden

☐ in het kader van gerechtelijke opdrachten

☐ geen specifieke reden

☐ andere ……

Ga daarom na welke types van gegevensverwerking u uitvoert en op basis van welke grondslag dit geschiedt zoals voorzien in de AVG.

U verwerkt persoonsgegevens aangezien:

☐de betrokkene **toestemming** heeft gegeven; voorbeeld: betrokkene heeft zich ingeschreven om de e-nieuwsbrief van het bedrijf te ontvangen en waarbij u betrokkene gewezen heeft op uw privacybeleid..

☐de verwerking **noodzakelijk is voor de uitvoering van een overeenkomst**; bv. indien een klant facturen brengt om te verwerken in de boekhouding, dan mag u uiteraard de persoonsgegevens die op de facturen zouden voorkomen verwerken. Of bv. indien een klant online betaalt, dan mag u uiteraard de kredietkaartgegevens verwerken om betaling te bekomen.

☐De verwerking **noodzakelijk** is om te voldoen aan een **wettelijke verplichting**:

- ☐als u werkgever bent, dan moet u gegevens over werknemers doorgeven aan de sociale zekerheid. (DIMONA)
- ☐ Fiscaal : BTW-listing, fiscale fiches, PB
- ☐Anti witwas wetgeving

☐Andere wettelijke verplichtingen:

In de AVG-regelgeving worden nog een aantal andere grondslagen vermeld[4] voor het verwerken.

Stap 3 – Pas op voor gevoelige persoonsgegevens !!

De verwerking van gevoelige persoonsgegevens is in beginsel **verboden** (art. 9 AVG). :

Gevoelige gegevens zijn : ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, het lidmaatschap van een vakbond, verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid

Doch op het verbod om deze gegevens te verwerken zijn een aantal **uitzonderingen** zoals[5]:

❖ In het geval van uitdrukkelijke toestemming van de betrokkene;

❖ Om te voldoen aan een wettelijke verplichting;

❖ Ter bescherming van de vitale belangen;

In concreto : Het kan zijn dat uw boekhouder kennis krijgt van gevoelige gegevens: voorbeelden: u doet de aangifte PB van iemand die lid is van een vakbond of voor partij X in de gemeenteraad zetelt of u doet de aangifte PB van een homoseksueel koppel.Hij is verantwoordelijk voor de boekhouding van een lokale politieke partij. Hij bewaart kopie van de e-id of van paspoorten met biometrische gegevens. Hij verwerkt de boekhouding van een arts en krijgt dus aldus zicht op diens patiënten.

Check dit hier voor uw bedrijf, vink aan en vul aan:

☐ Ik verwerk gevoelige gegevens:

Ik val onder één van vermelde uitzonderingen: zoals

☐Wettelijke verplichting : AWW/ WIB (belastingaangifte)

Ook het verwerken van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten kan enkel onder bepaalde voorwaarden (art. 10). Ik verwerk persoonsgegevens betreffende strafrechtelijke veroordelingen:

---

[4] ☐de verwerking **noodzakelijk is om de vitale belangen** van de betrokkene of een andere persoon te beschermen;

☐de verwerking **noodzakelijk is voor de vervulling van een taak van algemeen belang;**

☐de verwerking **noodzakelijk is voor de behartiging van een gerechtvaardigd belang.** o bv. gezondheidsdoeleinden zoals volksgezondheid, sociale bescherming, fraudevoorkoming, direct marketing, ...

[5] Andere zijn : Persoonsgegeven die kennelijk door de betrokkene openbaar zijn gemaakt; Wanneer het noodzakelijk is om een rechtsvordering in te stellen of wanneer een gerecht handelt binnen zijn rechtsbevoegdheid; Noodzakelijk om redenen van zwaarwegend algemeen belang (evenredigheid met het nagestreefde doel wordt gewaarborgd!); Noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid van de werknemer, medische diagnosen, het verstrekken van gezondheidszorg of sociale diensten; Noodzakelijk om redenen van algemeen belang op vlak van volksgezondheid; Noodzakelijk met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

JA ☐ / NEE ☐

Stap 4 – Vraagt u op een correcte manier toestemming?

Tenzij er een andere rechtmatige grondslag (zie stap 2) bestaat zal u voor het verwerken van persoonsgegevens de toestemming aan de betrokkene moeten vragen. Dit zal bv het geval zijn wanneer uw bedrijf persoonsgegevens wil verzamelen met oog op het versturen van een e-nieuwsbrief, het uitnodigen voor events zoals seminaries,...

Het vragen om toestemming is een zeer belangrijke handeling in de AVG. Volgens de AVG-regelgeving moet toestemming **vrij, specifiek, geïnformeerd en ondubbelzinnig** zijn. Toestemming moet ook steeds een duidelijk actieve handeling zijn (art. 4, 11° en art. 7 AVG). Dus het voorzien van een veld in een contactformulier op uw website met een daarin vooraf aangevinkt vakje wordt dus best vermeden.

Check dit hier voor uw kantoor, vink aan en vul aan:

- ☐ Ik voorzie bij de toestemming een vrijwillige keuze; waarbij de betrokkene uitdrukkelijk kan instemmen (een 'opt-in').
- ☐ Ik licht de betrokkene duidelijk in waarvoor en voor welke doeleinden toestemming wordt gegeven (cfr. recht op informatie).
- ☐ Ik leid geen toestemming af uit een stilzwijgen, een vooraf aangevinkt vakje of uit een niet-handelen.
- ☐ Ik voorzie de mogelijkheid dat de betrokkene te allen tijde zijn toestemming kan intrekken. Het intrekken van de toestemming is even eenvoudig als het geven van de toestemming. De uitschrijfmogelijkheden zijn duidelijk weergegeven.

Belangrijk is ook dat de toestemming steeds controleerbaar moet zijn. Dat wil zeggen dat u moet kunnen aantonen door wie, wanneer en hoe er toestemming werd gegeven. U registreert dit best in een document bv via de logs van de website of een systeem van e-sign.

□ De toestemming is controleerbaar.

Opgelet: Kinderen -16 !

Indien u persoonsgegevens verwerkt van kinderen onder de 16 jaar, dan zal een ouder of voogd toestemming moeten geven (art. 8 AVG). Deze verplichting geldt echter enkel wanneer de verwerking is gebaseerd op toestemming én wanneer het gaat om aangeboden diensten van de informatiemaatschappij (bv sociale netwerken).

Deze bepaling doet geen afbreuk aan het Belgische verbintenissenrecht (bv. de regels inzake de geldigheid, de totstandkoming of de gevolgen van overeenkomsten ten opzichte van kinderen).

U moet bovendien kunnen bewijzen dat u redelijke inspanningen heeft gedaan om de toestemming te verifiëren.

Check dit hier voor uw bedrijf :

☐ Ik bewaar gegevens van kinderen -16 gebaseerd op toestemming.

☐ Ik hanteer een systeem waardoor ik de toestemming kan verifiëren bij de ouders/voogd.

Wat met toestemmingen uit het verleden?

U dient geen nieuwe toestemming te vragen wanneer de eerder verkregen toestemming voldoet aan de nieuwe eisen. is dit niet her geval, dan moet u opnieuw en op een correcte wijze de toestemming vragen.

In het model van privacybeleid zit een toestemmingsclausule verwerkt.

Stap 5 – Garandeert u de rechten van de betrokkenen?

U moet als bedrijf rekening houden met heel wat rechten die de AVG verleent aan betrokkenen. Maak een nauwkeurige evaluatie en ga na waar u eventueel de nodige aanpassingen dient te doen. Het is belangrijk om te weten hoe u voortaan te werk zal gaan wanneer iemand zijn recht wil uitoefenen; wie is hiervoor verantwoordelijk? Weet die persoon wat te doen? Is het technisch mogelijk?

Uitgangspunt: betrokkenen dienen via een duidelijke **communicatie** geïnformeerd te worden over de regels voor de uitoefening van hen rechten (art. 12 AVG)

Alle informatie én communicatie moet enerzijds in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm, en anderzijds in duidelijke en eenvoudige taal worden verzorgd.

U maakt hiervoor best gebruik van een **"privacybeleid"** waarin u deze rechten opneemt en waarin u toelicht op welke wijze deze rechten kunnen worden uitgeoefend.

Deze rechten zijn altijd van toepassing tenzij wettelijke bepalingen hier in een uitzondering voorzien. Het is belangrijk dat u dit in uw privacybeleid uitdrukkelijk opneemt. **In bijlage vindt u een model van privacybeleid**.

Voor de **niet Anti witwas gerelateerde gegevens** (bv. de personen die u uitnodigt voor uw events) is het volgende integraal van toepassing :

Indien een betrokkene zich op een recht beroept, dan moet u binnen een maand na ontvangst van het verzoek reageren. Afhankelijk van de complexiteit van het verzoek kan die termijn worden verlengd met nog eens 2 maanden.

Check hieronder of u deze rechten effectief verleent in uw bedrijf en vink ze aan of duid aan als ze niet van toepassing zijn:

□ **Recht op informatie** (art. 13 en 14 AVG)

☐Ik verwerk geen persoonsgegevens zonder medeweten van betrokkenen.

☐Ons privacybeleid staat op de website

☐Ons privacybeleid is een bijlage bij onze algemene voorwaarden

☐Ons privacybeleid wordt toegelicht en medegedeeld bij het eerste contact

In de verordening is bepaald welke informatie aan uw klant moet worden meegedeeld, bv via een privacybeleid. Deze verplichting geldt ongeacht of de gegevens door de klant zelf werden vertrekt dan wel onrechtstreeks werden verkregen.

□ **Recht van inzage** (art. 15 AVG)

De persoon van wie u gegevens bijhoudt, heeft het recht om bepaalde gegevens in te zien en bijkomende informatie te ontvangen over heel wat zaken. Ik voorzie ook een gratis kopie van de verwerkte persoonsgegevens binnen de maand (verlengbaar met 2 maanden).

□ **Recht op correctie** (art. 16 AVG)

De persoon van wie u gegevens bijhoudt heeft het recht om onjuiste of onvolledige persoonsgegevens te verbeteren.

□ **Recht op verwijdering / recht om vergeten te worden** (art. 17 AVG)

In een aantal specifieke gevallen kan de persoon van wie u gegevens bijhoudt, vragen om 'vergeten te worden' en te worden verwijderd uit uw database.

U kan de vraag tot verwijdering ook weigeren in een aantal gevallen. In artikel 17 van de verordening wordt opgelijst wanneer dit mogelijk is.

□ **Recht op beperking** (art. 18 AVG)

In een aantal gevallen kan de betrokkene vragen om de draagwijdte van de verwerkte persoonsgegevens te beperken.

□ **Recht op overdraagbaarheid** van gegevens (art. 20 AVG)

De persoon van wie u gegevens verwerkt, heeft het recht om persoonsgegevens die hij heeft verstrekt, te laten overdragen aan een andere onderneming. De gegevens moeten gratis worden overgedragen, binnen een tijdspanne van een maand (verlengbaar met 2 maanden), in een gestructureerde gangbare en elektronisch leesbare vorm. Dit kan enkel voor gegevens die u verwerkt via een geautomatiseerd procedé en u op basis van toestemming of overeenkomst werden verstrekt.

□ **Recht van bezwaar** (art. 21 AVG)

De persoon van wie u gegevens verwerkt, heeft ten alle tijde het recht omwille van zijn specifieke situatie zich te verzetten tegen de verwerking van zijn gegevens (tenzij wettelijk bepaald of wanneer noodzakelijk voor uitvoeren van een overeenkomst). Wanneer gegevens worden verzameld met oog op direct marketing (incl. profiling die betrekking heeft op direct marketing) kan de betrokken persoon zich kosteloos en zonder verantwoording verzetten tegen de verwerking van zijn gegevens.

. □ **Geautomatiseerde besluitvorming**, waaronder profiling (art. 22 AVG)

Elke persoon van wie u gegevens bijhoudt, heeft het recht om niet te worden onderworpen aan een volledig geautomatiseerde besluitvorming. Het recht geldt niet wanneer de besluitvorming 1) nodig is om een overeenkomst te sluiten of uit te voeren; 2) wettelijk is toegestaan; 3) gebaseerd is op uitdrukkelijke toestemming.

Databeveiliging en toegangsbeperkingen	JA	NEE	NVT

Stap 6 computert u veilig ?

De AVG verplicht u in de eerste plaats om uw eigen infrastructuur en databanken goed te beveiligen.
Onderstaand vindt u alvast een basis ICT checklist :

	Gegevens inzake overheidsidentificatienummers, medische profielen en andere gevoelige gegevens worden met encryptie opgeslagen			
	De organisatie heeft een uitgeschreven en up to date dataregister			
	Voor bedrijven die zelf programma's ontwikkelen wordt persoonlijke informatie in de ontwikkelings- of testomgeving geanonimiseerd			
	Toestellen worden bij niet gebruik steeds locked achtergelaten			
	De netwerken worden gescheiden gehouden (aparte VLAN)			
	Toegang tot de applicatiesoftware wordt gelimiteerd op basis van gebruiker en in functie van de noodzaak om toegang te hebben			
	Toegang tot de data (mappen) wordt beperkt tot de bevoegde personen			
	Er zijn restricties en controle op de beperkte fysische toegang van personeel en derden tot datacenter en gevoelige technische ruimtes			
	Datacenter en gevoelige technische ruimtes zijn beschermd tegen onbevoegde toegang			
	Mediadragers die niet meer worden gebruikt worden vernietigd (HDD, CD, DVD, Tape,…)			
	Bij informatiebeveiligingsincidenten wordt gereageerd conform de uitgeschreven procedures			
	Medewerkers hebben een computer policy onderschreven waarin hun gebruik van aanwezige hard- & software geregeld wordt			
	Elke gebruiker heeft een individuele login en persoonlijk geheim wachtwoord			
	Het wachtwoordbeleid legt aan elke gebruiker een periodieke wijziging van paswoord op			
	Elk toestel start op met login en wachtwoord			
	Externe personen krijgen enkel op beveiligde wijze toegang (VPN, outlook anywhere,…) en dan ook enkel voor de voor hen noodzakelijke gegevens			

	Wifi netwerk is beveiligd met een sterk paswoord			
	Bezoekers loggen in via een afzonderlijk WIFI netwerk dat niet verbonden is met het bedrijfsdata netwerk			
	Er bestaat een cultuur van awareness : Gebruikers zijn bewust van de gevaren van malware en zijn voldoende op de hoogte van preventief werken			
	De informaticaperimeter is beschermd door firewall(s)			
	De geïnstalleerde firewalls staan op laatste systeemversie			
	Er wordt een log bijgehouden van firewall evenementen en incidenten			
	Er is gepaste antivirus aanwezig op ALLE systemen (PC's en servers) in het netwerk			
	De antivirus voert regelmatig scans uit op ALLE systemen (PC's en servers) in het netwerk			
	Antivirus is steeds up to date (met minstens een dagelijkse update)			
	Antivirus staat op laatste versie en patchlevel			
	De meest recente Windows /OFFICE update versie staat steeds geïnstalleerd			

Stap 7 – Heeft u een Data Protection Officer (DPO) nodig?

Het aanstellen van een DPO[6] is volledig nieuw. Sommige bedrijven zullen een DPO, een soort preventieadviseur voor privacy, moeten aanstellen. Het is een persoon met zowel deskundige, juridische als praktische kennis inzake privacy, die de onderneming dient bij te staan bij het toezicht op de interne naleving van de AVG (art. 37-39 AVG).

Wanneer **moet** u altijd een DPO aanstellen?

Het hangt er van af. A priori zal deze verplichting vaak **niet van toepassing** zijn.

[6] De verordening spraakt hier van een “functionaris voor gegevensbescherming (=FG)” doch DPO is de meest gebruikte term

Zelfs als u niet verplicht zou zijn een DPO aan te stellen kan het toch nuttig zijn dat binnen uw kantoor één persoon aangeduid wordt die zich o.a. bezig houdt met de diverse privacyaspecten doch zonder dat u deze DPO noemt.

Er zijn echter twee situaties waarin de AVG de aanstelling van een DPO verplicht is :

- ☐ Bent u hoofdzakelijk belast met het verwerken van gevoelige gegevens (cfr. stap 2)?
- ☐ Bent u hoofdzakelijk belast met het verwerken van persoonsgegevens die regelmatige en stelselmatige observatie op grote schaal eisen?

Dit laatste geval is natuurlijk heel vaag. U moet dit interpreteren in die zin dat u persoonsgegevens verwerkt in het kader van uw core business. U doet bv. aan direct marketing, of profiling maakt deel uit van uw business. Daarenboven moet het gaan om een aanzienlijke hoeveelheid aan persoonsgegevens.

Stap 8 – Moet u een Data Protection Impact Assessment (DPIA) uitvoeren?

Sommige ondernemingen zullen krachtens AVG een DPIA, een soort veiligheidsaudit, moeten (laten) uitvoeren voor bepaalde verwerkingen. Op de website van de Privacycommissie of in de richtlijnen van Werkgroep 29 vindt u meer informatie over de DPIA. In het geval u een DPIA moet uitvoeren, laat u zich best begeleiden door een expert.

Stap 9 – Stel een register van de verwerkingsactiviteiten op - art 30 AVG

Elke onderneming die persoonsgegevens verwerkt, zal een **register van haar verwerkingsactiviteiten** moeten opmaken en actueel houden (art. 30 AVG).

Dit register moet minstens volgende gegevens bevatten:

- ☐ De naam en contactgegevens van de (gezamenlijke) verwerkingsverantwoordelijke, van de vertegenwoordiger van de verwerkingsverantwoordelijke en/of in voorkomend geval van de functionaris voor gegevensbescherming (DPO)
- ☐ De verwerkingsdoeleinden [zie stap 1]
- ☐ Enerzijds een beschrijving van de categorieën van betrokkenen en anderzijds van de categorieën van persoonsgegevens [zie stap 2]
- ☐ De categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt (onder meer ontvangers in derde landen of internationale organisaties) [zie stap 1]
- ☐ Indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist [zie stap 1]
- ☐ Indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen [zie stap 6]

☐ Indien van toepassing, doorgave van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, indien nodig de documenten waaruit een adequaat beschermingsniveau blijkt.

De Privacycommissie heeft een model van register voor verwerkingsactiviteiten ter beschikking gesteld. Een model opgesteld door FOD-economie kan u hier vinden. Dit modellen zijn geen officiele documenten. U mag dus een ander register gebruiken zolang het basisdoel behouden blijft: **een volledig overzicht bieden van de verrichte persoonsgegevensverwerkingen.**

Dit document is uiterst belangrijk daar het ook de basis vormt voor een eventule controle (bv na een klacht of datalek) door de GBA[7] (huidige Privacycommissie) om te kijken of de verwerker conform is.

Stap 10 – Maak een privacybeleid aan (art. 24.2 AVG)

Deze oefening is ook een goede gelegenheid om een privacybeleid op te maken of het bestaande (bv ISQC 1) te evalueren en de AVG-regelgeving erin te integreren.

Dit is de samenvatting van de vorige stappen welke u zal toelaten om aan al uw AVG-informatieverplichtingen te voldoen.

Dit document dient minstens het volgende te bevatten:

☐ uw gegevens als verwerkingsverantwoordelijke – gegevens DPO of ander privacyaanspreekpunt op kantoor [zie stap 7]

☐ De identiteit van de eventuele verwerker en de wijze waarop die de gegevens zal aanwenden; [zie stap 11]

☐ De wettelijke grondslagen voor gegevensverwerking; [zie stap 1]

☐ De termijnen gedurende dewelke u de informatie zal bijhouden; [zie stap 1]

☐ Of u de gegevens uitwisselt buiten de Europese Unie;

☐ De mogelijkheid voor de betrokkene om een klacht in te dienen bij de GBA (huidige Privacycommissie) indien hij/zij meent dat zijn/haar persoonsgegevens foutief worden verwerkt;

☐ De rechten voor de betrokkenen; [zie stap 5]

☐ De technische en organisatorische maatregelen die u zal nemen om in overeenstemming met de AVG-regelgeving te zijn;

☐ De doeleinden waarvoor de gegevens zullen worden verwerkt; [zie stap 1]

Belangrijk is dat u ook hier transparant bent (cfr. recht op informatie, art.13-14 AVG) door bv deze tekst op uw website ter beschikking te stellen.

In ieder geval dient u het privacybeleid zo beknopt mogelijk te formuleren in begrijpbare en duidelijke taal.

[7] Op 24 mei 2018 houdt de huidige Privacycommissie op te bestaan. De Gegevensbeschermingsautoriteit (GBA) zal vanaf 25 mei 2018 de rol overnemen.

Bijgaand vindt u een model privacybeleid.

Stap 11 - relatie met verwerkers (art. 28 AVG)

In uw hoedanigheid van gegevensverwerkingsverantwoordelijke dienen al uw contracten met werknemers (contacteer uw sociaal secretariaat), verwerkers (onderaannemers) AVG conform te zijn.

U kan als bedrijf een onderaannemer aanstellen om persoonsgegevens te verwerken. Die onderaannemer wordt in de verordening een 'verwerker' genoemd.

Onder de AVG moet u ook kunnen garanderen dat u werkt met 'veilige' bedrijven als onderaannemer. Ook in het geval u bepaalde activiteiten uitbesteedt, is het belangrijk te beoordelen of de veiligheidsmaatregelen die worden voorzien in de bestaande contracten toereikend zijn en voldoen aan de AVG-regelgeving.

Evalueer uw bestaande contracten met leveranciers, onderaannemers, … en breng tijdig de nodige aanpassingen aan.

□ Ik let er op dat ik altijd en overal geschreven contracten heb die de nodige garanties voorzien inzake veiligheid.

Stap 12 – wat te doen bij een data-lek? – Art 33-34 AVG

Indien u wordt geconfronteerd met een data-lek (bv. uw systeem werd gehackt en al uw data werd gestolen) dan heeft u een **meldingsplicht** (onverwijld en ten laatste binnen de 72 uur) nadat u kennis heeft genomen van de inbreuk.

- a) Meldingsplicht bij GBA (huidige Privacycommissie) (art. 33 AVG)

U moet de GBA op de hoogte brengen binnen de 72 uur van een inbreuk wanneer die inbreuk vermoedelijk een risico vormt voor de rechten en vrijheden van natuurlijke personen. U moet enkel de inbreuken melden waarbij de kans groot is dat het schade zal berokkenen aan de persoon in kwestie. Bv. identiteitsdiefstal, schending geheimhoudingsplicht, …

- b) Meldingsplicht bij de betrokkene (art. 34 AVG)

Wanneer de inbreuk een hoog risico zou kunnen vormen voor de rechten en vrijheden van de betrokken personen, dan moeten die onverwijld worden gewaarschuwd. Bv. indien niet-geëncrypteerde bankgegevens werden gestolen.

De meldplicht ten aanzien van de betrokkene geldt niet in volgende gevallen:

❖ U heeft reeds passende technische en organisatorische beschermingsmaatregelen genomen met betrekking tot die gegevens (bv. versleuteling).

❖ U heeft achteraf maatregelen genomen om ervoor te zorgen dat het risico zich niet meer zal voordoen.

❖ Indien de meldplicht onevenredige inspanningen zou vergen (er moet dan wel een openbare mededeling gebeuren of een even doeltreffende soortgelijke maatregel genomen worden).

De melding ten aanzien van de GBA (huidige Privacycommissie) en de betrokkene moet minsten een aantal gegevens bevatten; zie specifieke webpagina Privacycommisie. U bent ook verplicht om alle inbreuken die zich hebben voorgedaan nauwkeurig bij te houden in een document.

Pas dit concreet toe op uw bedrijf :

□ Stel iemand aan die verantwoordelijk is voor controleren en melden van inbreuken:
…….

□ Bereid een template voor om inbreuken te melden

Probeer vooraf een inschatting te maken van het risico voor de rechten en vrijheden van personen indien u – op welke manier dan ook – de persoonsgegevens verliest. Afhankelijk van deze inschatting bereidt u zich al dan niet in betere mate voor op een mogelijke inbreuk. We raden u aan om dit na te vragen bij uw ICT-verantwoordelijke of ICT-leverancier

MODELTEKST PRIVACY BELEID

Bij voorkeur op te nemen in uw algemene voorwaarden, op uw website en bij inschrijving door clienten op nieuwsbrieven

Als onderneming staan wij in voor de verwerking van heel wat gegevens. Een deel van deze gegevens hebben betrekking op persoonsgegevens. In dit kader delen wij u het volgende mee.

De persoonsgegevens die wij verwerken kunnen betrekking op u in uw hoedanigheid van klant van onze onderneming maar ook op u als zakelijke relatie van onze klanten (zoals het geval dat u leverancier of klant bent van onze klant). In elk geval dienen wij u als **betrokkene** van wie persoonsgegevens door ons verwerkt worden op het volgende te wijzen.

1. Verantwoordelijke voor de verwerking van de persoonsgegevens.

De verantwoordelijke voor de verwerking van de persoonsgegevens is dhr <S>contact_naam</S>
De zetel van de verantwoordelijke is gelegen op de maatshappelijke zetel van onze vennootschap.
Voor alle vragen met betrekking tot de bescherming van persoonsgegevens, kunt u steeds terecht bij via brief aan ons bedrijf of via e-mail <S>contact_email</S>

2. Doeleinden van de verwerking van persoonsgegevens.

Onze onderneming verwerkt de persoonsgegevens voor de volgende doeleinden:

A. Toepassing van de Wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten.

1° In toepassing van het artikel 26 van de wet van 18 september 2017 dient ons kantoor met betrekking tot onze cliënten en hun lasthebbers de volgende persoonsgegevens in te winnen :de naam, de voornaam, de geboortedatum en -plaats en, in de mate van het mogelijke, het adres

2 ° In toepassing van het artikel 26 van de wet van 18 september 2017 dient ons kantoor betreffende de uiteindelijke begunstigden van de cliënten volgende persoonsgegevens in te winnen : de naam, de voornaam en in de mate van het mogelijk, de geboortedatum en -plaats en adres

De verwerking van deze persoonsgegevens is een wettelijke verplichting. Zonder deze gegevens kunnen wij niet overgaan tot het aangaan van een zakelijke relatie (art.33 Wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten.).

B. De op ons bedrijf rustende verplichtingen ten aanzien van de Belgische overheid, van buitenlandse overheden of van internationale instellingen in uitvoering van een wettelijke of reglementaire verplichting, in uitvoering van een gerechtelijke beslissing, of in het kader van de behartiging van een rechtmatig belang door o.a. doch niet uitsluitend de huidige en toekomstige fiscale (bv BTW-listings, fiscale fiches) en sociale wetten noodzaken ons om in het kader van de opdracht waarmee we werden belast persoonsgegevens te verwerken.

De verwerking van deze persoonsgegevens is een wettelijke verplichting en zonder deze gegevens kunnen wij niet overgaan tot het aangaan van een zakelijke relatie.

C. Uitvoering van onze overeenkomst betreffende de diensten en goederen die wij u aanbieden. De verwerking van de persoonsgegevens betreft de gegevens van de cliënten zelf, hun personeelsleden, hun bestuurders en dergelijke, alsook van de andere personen die o.a. als klant of leverancier betrokken zijn bij de activiteit.

Zonder de verstrekking en verwerking van deze gegevens kunnen wij onze opdracht als xxxxx niet naar behoren uitvoeren.

D. *het versturen van een maandelijkse nieuwsbrief per e-mail / post over onze bedrijfsactiviteitn en commerciele voorstellen.*

De in dit kader medegedeelde gegevens worden voor geen enkele andere doelstelling gebruikt.

3. Welke persoonsgegevens en van wie ?

In het kader van de onder 2 vermelde doeleinden kan ons bedrijf de volgende persoonsgegevens verwerken: voornaam, naam, e-mailadres, biometrische gegevens (kopie e-id of paspoort), adres, ondernemingsnummer nationaal nummer, huwelijksstatus, identiteit, leeftijd en aantal kinderen

Wij verwerken de persoonsgegevens welke de betrokkenen zelf of hun aanverwanten hebben aangeleverd. Onze ondernemin g verwerkt ook persoonsgegevens die niet door de betrokkene zelf werden aangebracht zoals xxx.

De persoonsgegevens kunnen ook afkomstig zijn van openbare bronnen zoals de Kruispuntenbank Ondernemingen, het Belgisch Staatsblad en de bijlagen ervan, de Nationale Bank van België (Balanscentrale) en dergelijke.

De gegevens worden slechts verwerkt voor zover noodzakelijk voor de onder punt 2 vermelde doeleinden. De persoonsgegevens worden niet doorgegeven aan derde landen of internationale organisaties.

4.Ontvanger van gegevens

Overeenkomstig wat voorafgaat en behalve in de mate dat de mededeling van persoonsgegevens aan organisaties of entiteiten wiens tussenkomst als third service providers voor rekening en onder de controle van de verantwoordelijke vereist is om de voormelde doeleinden te verwezenlijken, zal ons bedrijf de in dit kader verzamelde persoonsgegevens niet meedelen, verkopen, verhuren of uitwisselen met enige andere organisatie of entiteit, tenzij u daar op voorhand van op de hoogte werd gebracht en hiermee uitdrukkelijk mee instemde.

Ons bedrijf doet een beroep op volgende third service providers:

- Wij maken momenteel gebruik van volgende cloud software :
- Ons bedrijf doet , wanneer beroepsmatig vereist, een beroep op externe medewerkers voor het uitvoeren van bepaalde taken of specifieke opdrachten (bedrijfsrevisor, notaris, advokaat …)

Ons bedrijf zal alle redelijke maatregelen nemen die nodig zijn om een goed beheer van onze website en informaticasysteem te verzekeren.

Ons bedrijf kan de persoonsgegevens doorgeven op vraag van elke wettelijk bevoegde overheid, of zelfs op eigen initiatief indien ze te goeder trouw van oordeel is dat het doorgeven van die inlichtingen nodig is om aan de wetgeving en aan de reglementering te voldoen, of om de rechten of de goederen van het kantoor, van haar klanten, van haar website en/of van U te verdedigen en/of te beschermen.

5. Veiligheidsmaatregelen.

Teneinde, in de mate van het mogelijke, de ongeoorloofde toegang tot de in dit kader verzamelde persoonsgegevens te beletten, heeft ons bedrijf procedures op het gebied van veiligheid en organisatie opgesteld, welke betrekking hebben zowel op het verzamelen van deze gegevens als op hun bewaring.

6. Bewaringstermijn

6.1. Persoonsgegevens die wij moeten bewaren krachtens een Wet

6.2.Andere persoonsgegevens

De persoonsgegevens van de andere dan hierboven vermelde personen worden slechts bewaard gedurende de termijnen zoals voorzien in de toepasselijke wetgeving zoals de boekhoudwetgeving, de fiscale wetgeving, de sociale wetgeving.

6.3 Na het verstrijken van de voormelde termijnen worden de persoonsgegevens gewist, tenzij een andere geldende wetgeving een langere bewaartermijn voorziet.

7. Rechten van toegang, rectificatie, vergeteldheid, gegevensoverdraagbaarheid, bezwaar, niet-profilering en betreffende kennisgeving veiligheidsgebreken

7.1. Betreffende de persoonsgegevens die wij moeten bewaren in toepassing van de Wet van 18 september 2017.

Dit betreft de persoonsgegevens van onze cliënten, de lasthebbers en de uiteindelijke begunstigden van de cliënten.

Ter zake dienen wij u te wijzen op het artikel 65 van de wet van 18 september 2017 :

“Art. 65. De persoon op wie krachtens deze wet de verwerking van de persoonsgegevens van toepassing is, geniet niet van het recht op toegang en de rechtzetting van zijn gegevens, noch van het recht om vergeten te worden, op gegevensoverdraagbaarheid of om bezwaren aan te voeren, noch van het recht om niet geprofileerd te worden, noch van kennisgeving van de veiligheidsgebreken.

Het recht op toegang van de betrokken persoon tot de persoonsgegevens die hem aangaan, wordt onrechtstreeks uitgeoefend, krachtens het artikel 13 van de voornoemde wet van 8 december 1992, bij de Commissie voor de Bescherming van de Persoonlijke Levenssfeer zoals ingesteld door artikel 23 van dezelfde wet.

De Commissie voor de bescherming van de persoonlijke levenssfeer deelt uitsluitend aan de verzoeker mede dat de nodige verificaties werden verricht en over het resultaat daarvan wat de rechtmatigheid van de verwerking in kwestie betreft.

Deze gegevens kunnen worden meegedeeld aan de verzoeker wanneer de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, in samenspraak met de CFI en na advies van de verantwoordelijke voor de verwerking, enerzijds vaststelt dat de mededeling ervan niet vatbaar is voor bekendmaking van het bestaan van een melding van een vermoeden bedoeld in de artikelen 47 en 54, van de gevolgen die hieraan werden gegeven of van de uitoefening door de CFI van haar recht om bijkomende inlichtingen te vragen op grond van artikel 81, noch vatbaar is om de doelstelling van de strijd tegen WG/FT in het gedrang te brengen, en anderzijds vaststelt dat de betreffende gegevens betrekking hebben op de verzoeker en door onderworpen entiteiten, de CFI of de toezichtautoriteiten worden bijgehouden voor toepassing van deze wet."

Voor de toepassing van uw rechten inzake uw persoonsgegevens dient u zich dus te wenden tot de de of Gegegevensbeschermingsautoriteit (zie punt 8.)

7.2. Alle andere persoonsgegevens

Voor de toepassing van uw rechten betreffende alle andere persoonsgegevens kan u steeds contact nemen met <S>contact_naam</S>

8. Klachten

Inzake de verwerking van de persoonsgegevens door ons bedrijf kan U een klacht indienen bij de Gegevensbeschermingsautoriteit :

Commissie voor de bescherming van de persoonlijke levenssfeer

Drukpersstraat 35, 1000 Brussel

Tel +32 (0)2 274 48 00

Fax : +32 (0)2 274 48 35

E-mail : commission@privacycommission.be

URL: https://www.privacycommission.be