GDPR CHECKLIST

Wij zetten uw onderneming op weg naar PRIVACY compliance!

Volg de 10 stappen in deze leidraad, vul ze in en stel u zo in orde met de nieuwe privacyregels

Stap 1 – Breng uw data in kaart

Het opmaken van een soort 'data-inventaris' is een eerste zeer belangrijke stap in uw voorbereiding. U moet proberen in kaart te brengen welke data u allemaal verwerkt[1]. U kan deze oefening bijvoorbeeld maken in een Excel bestand. Hiermee kan u bewijzen dat u de oefening heeft gemaakt, maar bovendien draagt het bij aan de maturiteit van uw onderneming.

Overloop onderstaande vragen. Ze helpen u om zicht te krijgen op uw data-instroom.

☐ Van wie houdt u persoonsgegevens bij?
- ☐ Klanten
- ☐ Leveranciers
- ☐ Personeel
- ☐ Prospecten
- ☐ Andere: ……

☐ Welke categorieën van persoonsgegevens houdt u bij?
- ☐ Identiteitsgegevens (naam, adres, telefoonnummer, …)
- ☐ Facturatiegegevens
- ☐ Gevoelige gegevens (gezondheid, geaardheid, …)
- ☐ Andere: ……
  ……

☐ Waar komen deze persoonsgegevens vandaan?

……

……

<u>Opgelet:</u> Volgens de GDPR mag u enkel samenwerken met 'veilige' bedrijven. Het is belangrijk dat u deze garantie voorziet in de contracten met uw partners.

☐ Waar slaat u deze persoonsgegevens op? In welke databank(en) en waar bevind(t)(en) die zich?

……

……

[1] 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.

☐ Wie heeft er allemaal toegang tot deze databank? Welke functies hebben deze personen?

……

……

Is het wel noodzakelijk dat bepaalde mensen toegang hebben tot deze databank? Is de toegang beveiligd? Neem de nodige maatregelen om beveiliging te voorzien. Dit kan een digitale beveiliging zijn, maar evenzeer een slot op de kast waar bepaalde documenten worden bewaard.

☐ Worden deze persoonsgegevens gedeeld of overgedragen aan een andere onderneming? Binnen of buiten de EU (cloud)?

……

……

Opgelet: Indien u bv. een persoonsgegeven corrigeert dan zal u de onderneming aan wie u gegevens overdraagt op de hoogte moeten brengen van deze correctie.

Doorgiften naar landen buiten de EU is enkel mogelijk indien aan alle voorwaarden en verplichtingen inzake doorgifte is voldaan (o.a. art. 13.1 e); art. 14.1 f); art. 15.2; art. 30.1 e); art. 44-50; …).

☐ Waarom houdt u deze persoonsgegevens bij?

……

……

*Opgelet: U mag enkel persoonsgegevens verzamelen voor welbepaalde, uitdrukkelijk omschreven en **gerechtvaardigde doeleinden**. De persoonsgegevens moeten relevant en beperkt zijn tot de beoogde doeleinden van de verwerking (zie verder).*

☐ Hoelang houdt u de gegevens bij?

……

……

Opgelet: De persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk voor de beoogde doeleinden van de verwerking.

De uitkomst van deze oefening zal u helpen in het verdere proces om uw onderneming privacy compliance te maken. Voornamelijk in stap 9 zal deze eerste stap van pas komen.

Stap 2 – Denk na over de wettelijke grondslag voor het verwerken van persoonsgegevens

U mag enkel persoonsgegevens verzamelen en verwerken wanneer daarvoor een wettelijke grondslag bestaat (art. 6).

Ga daarom na welke types van gegevensverwerking u uitvoert en op basis van welke wettelijke grondslag. Vink ze hieronder aan:

U verwerkt persoonsgegevens aangezien:

- ❑ de betrokkene **toestemming** heeft gegeven;
- ❑ de verwerking noodzakelijk is voor de **uitvoering van een overeenkomst**;
  - *bv. indien een klant iets bestelt en u moet dit leveren, dan mag u uiteraard het adres van die persoon verwerken.*
  - *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**;
  - *bv. als u werkgever bent, dan moet u gegevens over werknemers doorgeven aan de sociale zekerheid.*
- ❑ 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**.
  - *bv. gezondheidsdoeleinden zoals volksgezondheid, sociale bescherming, fraudevoorkoming, direct marketing, …*
  - *In elk geval zal er steeds een belangenafweging moeten worden gemaakt (overweging 47).*

Waarom is het nu zo belangrijk om te weten?

Afhankelijk van de wettelijke basis kunnen de rechten van de betrokkene variëren. Zo heeft de betrokkene bv. een sterker recht om de verwijdering van zijn gegevens te vragen indien de persoonsgegevens werden verwerkt op basis van zijn/haar toestemming (stap 4).

De wettelijke grondslag dient ook verduidelijkt te worden in de Privacy Policy en telkens wanneer u een recht op toegang beantwoordt (zie hier).

Stap 3 – Pas op voor gevoelige persoonsgegevens

De verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en 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 zijn **verboden** (art. 9).

Hierop zijn een aantal **uitzonderingen**:

- In het geval van uitdrukkelijke toestemming van de betrokkene;
- Om te voldoen aan een wettelijke verplichting;
- Ter bescherming van de vitale belangen;
- 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.

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

☐ Ik verwerk gevoelige gegevens: …… …… …… ……
……

☐ Ik val onder een uitzondering: ……
……

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

☐ Ik verwerk persoonsgegevens betreffende strafrechtelijke veroordelingen: ……
……

Indien u bovenstaande gegevens verwerkt, dan verwijzen wij u graag door naar de website van de Privacy commissie waar u meer info vindt over gevoelige persoonsgegevens en gegevens over strafrechtelijke veroordelingen. Het is mogelijk dat u in dit geval best contact opneemt met een professional.

Stap 4 – Vraagt u op een correcte manier toestemming?

Het vragen om toestemming is een zeer belangrijke handeling in de GDPR. Volgens de GDPR moet toestemming *vrij, specifiek, geïnformeerd en ondubbelzinnig* zijn. Toestemming moet ook steeds een duidelijk *bevestigende handeling* zijn (art. 4, 11) en art. 7).

Check dit hier voor uw onderneming, 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 voor wat 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 ten allen tijde zijn toestemming kan intrekken. Het intrekken van de toestemming is even eenvoudig als het geven van de toestemming, bv. duidelijk weergeven van uitschrijfmogelijkheden.

Belangrijk is ook dat de toestemming steeds *controleerbaar* moet zijn. Dat wil zeggen dat u moet kunnen aantonen wie, wanneer en hoe er toestemming werd gegeven. U registreert dit best in een document.

- ☐ De toestemming is controleerbaar.

Opgelet: Kinderen -16!

Indien u als onderneming persoonsgegevens verzamelt en verwerkt van kinderen onder de 16 jaar, dan zal een ouder of voogd toestemming moeten geven (art. 8). Deze verplichting geldt enkel wanneer de verwerking is gebaseerd op toestemming én wanneer het gaat om aangeboden diensten van de informatiemaatschappij. De lidstaten kunnen echter bepalen om deze leeftijd nog lager te leggen (tot max. 13 jaar).

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 onderneming

- ☐ 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 toestemming uit het verleden?

U dient geen nieuwe toestemming te vragen wanneer de reeds verkregen toestemming voldoet aan de nieuwe eisen. Zoniet, moet u opnieuw op correcte wijze toestemming vragen.

Stap 5 – Garandeert u de rechten van de betrokkenen?

U moet als onderneming rekening houden met heel wat rechten die de GDPR 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?

Check hieronder of u deze rechten (correct) toepast in uw onderneming en vink ze aan of duid aan als ze niet van toepassing zijn:

☐ **CHECK: Duidelijke communicatie en nadere regels voor de uitoefening van de rechten van de betrokkene** (art. 12 GDPR)

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

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: Recht op informatie** (art. 13 en 14 GDPR)

Ik verwerk geen persoonsgegevens zonder medeweten van mijn klanten.

⇨ In de verordening is bepaald welke gegevens aan uw klant moeten worden meegedeeld. Deze verplichting geldt ongeacht of de gegevens bij de klant zelf of onrechtstreeks zijn verkregen.

⇨ Klik hier voor een overzicht van informatie die u aan betrokkene moet verstrekken.

☐ **CHECK: Recht van inzage** (art. 15 GDPR)

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).

⇨ Een modelantwoord vindt u hier.

☐ **CHECK: Recht op correctie** (art. 16 GDPR)

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

Ik breng iedere ontvanger aan wie ik persoonsgegevens heb verstrekt op de hoogte van een correctie, tenzij dit onmogelijk is of onevenredig veel inspanning vergt (kennisgevingsplicht art. 19).

☐ **CHECK: Recht op verwijdering / recht op vergetelheid** (art. 17 GDPR)

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. U vindt hier een lijst met enerzijds de gevallen tot verwijdering, anderzijds de gevallen waarin u dit verzoek kan weigeren.

Ik breng iedere ontvanger aan wie ik persoonsgegevens heb verstrekt op de hoogte van een verwijdering, tenzij dit onmogelijk is of onevenredig veel inspanning vergt (kennisgevingsplicht art. 19).

☐ **CHECK: Recht op beperking** (art. 18)

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

Ik breng iedere ontvanger aan wie ik persoonsgegevens heb verstrekt op de hoogte van een beperking, tenzij dit onmogelijk is of onevenredig veel inspanning vergt (kennisgevingsplicht art. 19).

☐ **CHECK: Recht op overdraagbaarheid van gegevens** (art. 20 GDPR)

De persoon van wie u gegevens bijhoudt, 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 de u als onderneming verwerkt via een geautomatiseerd procedé en op basis van toestemming of overeenkomst.

❑ niet van toepassing

☐ **CHECK: Recht van bezwaar** (art. 21 GDPR)

De persoon van wie u gegevens bijhoudt, 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.

❑ Ik informeer de betrokken persoon in elk geval van zijn recht op verzet en ik vermeld het uitdrukkelijk in de privacy policy.

☐ **CHECK: Geautomatiseerde besluitvorming, waaronder profiling** (art. 22 GDPR)

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.

Stap 6 – Bent u voorbereid op een data-lek?

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 of binnen de 72 uur) nadat u kennis heeft genomen van de inbreuk.

a) Meldingsplicht bij Privacy Commissie (art. 33 GDPR)

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

b) Meldingsplicht bij de betrokkene (art. 34 GDPR)

Wanneer de inbreuk *een hoog risico* zou kunnen vormen voor de rechten en vrijheden van de **betrokken personen**, dan moeten die onverwijld worden verwittigd. 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 doen of een even doeltreffende soortgelijke maatregel nemen).

De melding ten aanzien van de Privacy Commissie en de betrokkene moeten minsten een aantal gegevens bevatten; zie hier of op de website van de Privacy Commissie. U bent ook verplicht om alle inbreuken die zich hebben voorgedaan nauwkeurig bij te houden in een document.

Pas dit concreet toe op uw onderneming:

- ☐ 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 webmaster.

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

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

Wanneer moet u een DPO aanstellen?

Het hangt er van af. Er zijn twee situaties waarin de GDPR de aanstelling van een DPO verplicht aan ondernemingen:

- ☐ 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 als 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.

Bevindt u zich niet in één van deze gevallen, vink dan het vakje hieronder aan:

- ☐ Niet van toepassing

Wat doet zo'n expert precies?

- Een DPO geeft **informatie en advies** omtrent de GDPR-verplichtingen aan uw onderneming.
- Een DPO **monitort de naleving** van de GDPR.
- Een DPO is het **centrale aanspreekpunt** inzake gegevensbescherming (zowel voor de onderneming, voor de privacy commissie als voor personen wiens gegevens werden verwerkt).
- Een DPO **adviseert** de onderneming **omtrent** de verplichte **risicoanalyse** en de resultaten.

Aan wie mag u deze rol toekennen?

- Een **bestaande werknemer** met voldoende kennis inzake privacy. De professionele taken van de werknemer moeten combineerbaar zijn met de taken van een DPO. In geen geval mag dit leiden tot een belangenconflict.
- Een **externe** DPO, bv. een consultant, die deze taak enkele uren per week / maand uitvoert.

Meer info vindt u op de website van de Privacy Commissie of in de richtlijnen van werkgroep 29 (een Europese orgaan). Heeft u een DPO nodig, laat u dan bijstaan door een expert om u in orde te brengen met de GDPR.

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

Sommige ondernemingen zullen een DPIA, een soort veiligheidsaudit, moeten (laten) uitvoeren voor bepaalde verwerkingen.

Wanneer is een DPIA vereist?

Er zijn drie situaties waarin de GDPR dit verplicht:

- ☐ Wanneer u op geautomatiseerde wijze de persoonlijke kenmerken van personen systematisch beoordeelt (bv. profiling) en op basis van deze beoordeling acties onderneemt die rechtsgevolgen of een gelijkaardige impact hebben op deze personen (bv. direct marketing);
- ☐ In geval van grootschalige verwerking van bijzondere categorieën van persoonsgegevens of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten;
- ☐ In geval van stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

Voor veel zelfstandigen en KMO's zal deze assessment niet nodig zijn. Bevindt u zich niet in één van deze gevallen, vink dan het vakje hieronder aan:

- ☐ Niet van toepassing

Wanneer de DPIA aangeeft dat het verwerken van de persoonsgegevens een hoog risico inhoudt én indien u dat hoog risico niet kan beperken door maatregelen die met het oog op beschikbare technologie en de uitvoeringskosten redelijk zijn, moet u advies inwinnen van de Privacy Commissie en de nodige maatregelen nemen om het risico te bedwingen.

Deze verplichting geldt enkel voor **hoge risicosituaties**. De beoordeling van een 'hoog risico moet steeds gebeuren in functie van de soorten persoonsgegevens, de omvang en frequentie van de verwerking (art. 35-36). Bv. wanneer een nieuwe technologie wordt geïmplementeerd of wanneer een profileringsoperatie een aanzienlijk effect kan teweegbrengen voor de betrokkene.

Op de website van de Privacy Commissie 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

Stap 9 – Heeft u een register van de verwerkingsactiviteiten?

Elke onderneming die persoonsgegevens verwerkt, zal een register van haar verwerkingsactiviteiten moeten bijhouden (art. 30).

Vink hieronder aan om te checken of u hieraan voldoet.

Het register bevat volgende gegevens:

- ☐ In voorkomend geval, de **naam en contactgegevens** van de (gezamenlijke) verwerkingsverantwoordelijke, van de vertegenwoordiger van de verwerkingsverantwoordelijke en/of van de functionaris voor gegevensbescherming
- ☐ De **verwerkingsdoeleinden**
- ☐ Enerzijds een beschrijving van de **categorieën van betrokkenen** en anderzijds van de **categorieën van persoonsgegevens**
- ☐ De **categorieën van ontvangers** aan wie de persoonsgegevens zijn of zullen worden verstrekt (onder meer ontvangers in derde landen of internationale organisaties)
- ☐ Indien mogelijk, de **beoogde termijnen** waarbinnen de verschillende categorieën van gegevens moeten worden gewist
- ☐ Indien mogelijk, een algemene beschrijving van de **technische en organisatorische beveiligingsmaatregelen**
- ☐ Indien van toepassing, **doorgiften** 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 inzake de passende waarborgen.

De Privacy commissie heeft een model van register voor verwerkingsactiviteiten ter beschikking gesteld. Dit model is geen officieel document, u mag dus een ander Register gebruiken zelfs in een ander format (andere software, …) zolang het basisdoel van het Register behouden blijft: een volledig overzicht bieden van de verrichte persoonsgegevensverwerkingen.

Stap 10 – Pas uw privacy policy en contracten aan

Privacy policy (art. 24.2)

Deze oefening is ook een goede aangelegenheid om uw privacy policy te evalueren.

Om compliant te zijn met de GDPR voegt u hier best een aantal zaken aan toe:

- ☐ De identiteit van de verwerker en de wijze waarop die de gegevens zal aanwenden;
- ☐ De wettelijke grondslag voor gegevensverwerking;
- ☐ De termijnen gedurende dewelke u de informatie zal bijhouden;
- ☐ Of u de gegevens uitwisselt buiten de Europese Unie;
- ☐ De mogelijkheid voor de betrokkene om een klacht in te dienen bij de Privacy Commissie indien hij/zij meent dat zijn/haar persoonsgegevens foutief worden verwerkt;
- ☐ De rechten voor de betrokkenen;
- ☐ De technische en organisatorische maatregelen die u zal nemen om compliant te zijn;
- ☐ De doeleinden waarvoor de gegevens zullen worden verwerkt;
- ☐ …

Belangrijk is dat u ook hier **transparant** bent (cfr. recht op informatie, art.13-14). Bij het opstellen van uw privacy policy kan u zich laten leiden door de informatie die u dient te bezorgen wanneer u persoonsgegevens ontvangt (zie hier).

In ieder geval dient u de privacy policy zo beknopt mogelijk te formuleren in begrijpbare en duidelijke taal.

Contracten (art. 28)

Al uw contracten (met leveranciers, werknemers, verwerkers[2], …) dienen GDPR compliant te zijn.

Onder de nieuwe verordening moet u ook kunnen garanderen dat u werkt met 'veilige' bedrijven. De GDPR verplicht u in de eerste plaats om uw eigen databanken goed te beveiligen. Ook in het geval u bepaalde activiteiten uitbesteed, is het belangrijk te beoordelen of de veiligheidsmaatregelen die worden voorzien in de bestaande contracten toereikend zijn en voldoen aan de GDPR. Voor bestaande contracten kan u bv. een annex toevoegen.

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.

[2] U kan als onderneming een externe onderaannemer aanstellen om persoonsgegevens te verwerken. Die onderaannemer wordt in dat geval een 'verwerker' genoemd.

Na het doorlopen van deze checklist bent u normaal in voldoende mate privacy compliant. We raden u zeker aan om al uw stappen en acties goed te documenteren en te bewaren.

Naam: …….. **Datum:**……..

Onderneming:…… **Handtekening:** ……..

Meer info: www.unizo.be/privacy

UNIZO ONDERNEMERSLIJN
0800 20 750
ondernemerslijn@unizo.be