GDPR-TOOL

Zet 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

Versie maart 2018

unizo

Stap 1
Verwerkt u persoonsgegevens? Welke?

Zodra u ook maar iets van persoonsgegevens bijhoudt of verwerkt bent u aan de GDPR onderhevig.

Daarom is het van belang om eerst een overzicht te maken van welke gegevens u allemaal verzamelt en verwerkt.

- Ofwel gebruikt u **onderstaande checklist als voorbereiding** voor u zelf.
- Ofwel gaat u **onmiddellijk naar stap 2** en vult u het register van verwerkingsactiviteiten in.

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

Welke persoonsgegevens houdt u bij?
O Klanten
O Leveranciers
O Personeel
O Prospecten
O Andere:

Waar komen deze persoonsgegevens vandaan?

Opgelet: 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?

Wie heeft er allemaal toegang tot deze databank?

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?

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. .

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.

U kan deze voorbereiding gebruiken om uw Register van Verwerkingsactiviteiten effectief in te vullen (zie stap 2).

Stap 2
Leg een register van verwerkings-activiteiten aan

Dit is een heel belangrijke actie in het kader van de GDPR!
Bijna elke onderneming die persoonsgegevens verwerkt, zal een register van haar verwerkingsactiviteiten moeten bijhouden!

Download hier een invulbaar model van Register van Verwerkingsactiviteiten.

Hoe vult u dit in?
- Dit is een excel-bestand met 4 tabbladen. U moet enkel het tabblad 'Algemene info' en het tabblad 'Register' invullen.
- Als u in het tabblad 'Register' op een vakje klikt, verschijnt er rechts een pijltje, als u daar op klikt, kan u de categorie naar keuze aanduiden.
- In het tabblad 'Register' moet u de rechtsgrond (wettelijke grondslag) aanduiden: ga daarvoor naar stap 3.

Hieronder kan u nog eens overlopen en afvinken of u alles goed heeft ingevuld in uw Register:

Uw register moet volgende gegevens bevatten:

- ○ 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

Stap 3

Welke (wettelijke) grondslag heeft u voor het verwerken van persoonsgegevens?

U mag enkel persoonsgegevens verzamelen en verwerken wanneer daarvoor een wettelijke grondslag bestaat. Dat wil daarom niet zeggen dat u altijd verplicht de expliciete toestemming nodig heeft. Er zijn namelijk **zes grondslagen** die u toelaten om persoonsgegevens te verwerken (zie onderstaand kader).

U moet dit eveneens **invullen in uw Register Verwerkingsactiviteiten** (zie vorige stap 2).

Hieronder kan u ter voorbereiding of als check de zes grondslagen overlopen en afvinken welke types van gegevensverwerking u uitvoert en op basis van welke wettelijke grondslag.

U verwerkt persoonsgegevens aangezien:

O de betrokkene **toestemming** heeft gegeven;

O de verwerking noodzakelijk is voor de **uitvoering van een overeenkomst / contract**;
- *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.*

O 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.

O de verwerking noodzakelijk is om de **vitale belangen** van de betrokkene of een andere persoon te beschermen;

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

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

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.

De wettelijke grondslag dient ook verduidelijkt te worden in uw Privacy Policy en telkens wanneer u een recht op toegang beantwoordt.

Stap 4
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**.

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;
- Voor het uitvoeren van een taak van algemeen belang;
- ...

Check dit hier voor uw onderneming, vink aan en vul aan indien van toepassing. Indien dit niet van toepassing is voor uw activiteiten zet u gewoon een streep /

O Ik verwerk gevoelige gegevens:

O Ik val onder een uitzondering:

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

O 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 5
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.

Check dit hier voor uw onderneming en vink aan van toepassing is:

- O Ik voorzie bij de toestemming een vrijwillige keuze; waarbij de betrokkene uitdrukkelijk kan instemmen *(dit is een zogenaamde 'opt-in')*.
- O Ik licht de betrokkene duidelijk in voor wat en voor welke doeleinden toestemming wordt gegeven *(cfr. recht op informatie)*.
- O Ik leid geen toestemming af uit een stilzwijgen, een vooraf aangevinkt vakje of uit een niet-handelen.
- O 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.

- O De toestemming is controleerbaar.

OPGELET: Kinderen -13!

Indien u als onderneming persoonsgegevens verzamelt en verwerkt van kinderen onder de 13 jaar, dan zal een ouder of voogd toestemming moeten geven. Deze verplichting geldt enkel wanneer de verwerking is gebaseerd op toestemming én wanneer het gaat om aangeboden diensten van de informatiemaatschappij. U moet kunnen bewijzen dat u redelijke inspanningen heeft gedaan om de toestemming te verifiëren

Check dit hier voor uw onderneming: vink enkel aan indien van toepassing!

- O Ik bewaar gegevens van kinderen -13 gebaseerd op toestemming.
- O 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. Zo niet, dan moet u opnieuw op correcte wijze toestemming vragen.

Stap 6
Garandeert u de rechten van de betrokkenen?

U moet als onderneming rekening houden met heel wat rechten die de GDPR verleent aan betrokkenen van wie u gegevens verwerkt. Bent u van deze rechten op de hoogte en past u deze correct toe? Gebruik hiervoor onderstaande checklist.

Dit is een vrij omstandig onderdeel in het GDPR-proof maken van uw onderneming. Maar doe de checks, stap voor stap. Voor sommige van deze rechten komt het er gewoon op aan ze correct toe te passen.

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: "Recht op informatie" wordt correct toegepast**

→ U verwerkt geen persoonsgegevens zonder medeweten van uw klanten.

→ U deelt de volgende gegevens mee aan uw klant (wettelijk verplicht):
- uw naam en adres;
- het doeleinde van de verwerking (bv. "direct marketing");
- het bestaan van een kosteloos recht van verzet;
- het bestaan van een recht op toegang en verbetering;
- de ontvangers of de categorieën van ontvangers van de gegevens.

→ Deze verplichting geldt ongeacht of u de gegevens bij de klant zelf haalt of u ze onrechtstreeks verkregen heeft.

○ **CHECK: "Recht van inzage" wordt correct toegepast**

→ 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.

→ U voorziet ook een gratis kopie van de verwerkte persoonsgegevens binnen de maand (verlengbaar met 2 maanden).

→ Een modelantwoord aan een persoon die inzake vraagt, vindt u **hier**.

○ **CHECK: "Recht op correctie" wordt correct toegepast**

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

→ U reageert daarvoor binnen de maand (verlengbaar met 2 maanden).

→ U informeert ook derden aan wie deze gegevens werden bezorgd hierover en deelt aan de betrokkene mee aan welke derden de persoonsgegevens werden bezorgd.

○ **CHECK: "Recht op verwijdering" wordt correct toegepast**

→ 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 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.

○ **CHECK: "Recht op beperking" wordt correct toegepast**

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

- De betrokkene betwist de juistheid van de gegevens;
- De betrokkene heeft bezwaar gemaakt tegen de verwerking;
- In geval u onrechtmatig gegevens verwerkt is (beperking wordt gevraagd i.p.v. uitwissing)
- U heeft de gegevens niet langer nodig maar de betrokkene heeft ze zelf nodig

Zie **website** Privacy Commissie.

○ **CHECK: "Kennisgevingsplicht inzake correctie of verwijdering" wordt correct toegepast**

Als u een correctie, verwijdering of beperking van persoonsgegevens heeft doorgevoerd, brengt u iedereen **aan wie** u deze persoonsgegevens heeft doorgegeven op de hoogte hiervan. Dit is niet vereist als dit onmogelijk is of onevenredig veel inspanning vergt.

○ **CHECK: "Recht op overdraagbaarheid" van gegevens wordt correct toegepast**

→ De persoon van wie u gegevens bijhoudt, heeft het recht om persoonsgegevens die hij heeft verstrekt, te laten overdragen aan een andere verwerker.

→ Deze gegevens moete u gratis over dragen, binnen een tijdspanne van een maand (verlengbaar met 2 maanden), in gestructureerde gangbare en elektronisch leesbare vorm.

→ Dit kan enkel voor gegevens die de betrokken persoon heeft verstrekt op basis van toestemming of overeenkomst.

○ **CHECK: "Recht van verzet" wordt correct toegepast**

→ De persoon van wie u gegevens bijhoudt, heeft het recht zich te verzetten tegen de verwerking van zijn gegevens op basis van ernstige en gerechtvaardigde redenen.

→ Wanneer u gegevens verzamelt met oog op direct marketing en/of profiling kan de betrokken persoon zich kosteloos en zonder verantwoording verzetten tegen de verwerking van zijn gegevens.

- ○ U informeert de betrokken persoon in elk geval van zijn recht op verzet en u vermeldt het uitdrukkelijk in de privacy policy.

○ **CHECK: "Geautomatiseerde besluitvorming", waaronder profiling, wordt correct toegepast**

→ 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 1) de besluitvorming nodig is om een overeenkomst te sluiten of uit te voeren; 2) wettelijk is toegestaan; 3) gebaseerd is op uitdrukkelijke toestemming.

○ **CHECK: U gebruikt duidelijke communicatie en nadere regels voor de uitoefening van de rechten van de betrokkene**

→ 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.

Stap 7
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** nadat u kennis heeft genomen van de inbreuk.

A - Meldingsplicht bij Privacy Commissie

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. Bijvoorbeeld: identiteitsdiefstal, schending van geheimhoudingsplicht, ...

Opgelet! De aangifte MOET gebeuren via het webformulier op de website van de Privacy Commissie. Aangiftes per e-mail worden behandeld als vraag of als klacht. U loopt hierbij dan het risico dat u niet voldoet aan de meldingsplicht!

B - Meldingsplicht bij de betrokkene

Wanneer de inbreuk *een hoog risico* zou kunnen vormen voor de rechten en vrijheden van de **betrokken personen**, dan moeten ook de personen zelf **onverwijld** *(zo snel mogelijk dus!)* worden verwittigd. Bv. 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 voordoet
- Indien de meldplicht onevenredige inspanningen zou vergen. In dat geval moet u wel een openbare mededeling doen of een even doeltreffende soortgelijke maatregel nemen.

C - Verplichte gegevens bij melding data-lek

De melding ten aanzien van de Privacy Commissie en de betrokkene moeten minstens een aantal gegevens bevatten. 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:

O Stel iemand aan die verantwoordelijk is voor controleren en melden van inbreuken:

O Hou een modeldocument beschikbaar om een inbreuk te melden.
O Maak vooraf een inschatting van het risico voor de rechten en vrijheden van personen indien u – op welke manier dan ook – de persoonsgegevens verliest. We raden u aan om hiervoor af te stemmen met uw IT-beheerder

Stap 8

Heeft u een Data Protection Officer (DPO) nodig? Moet u een DPIA uitvoeren?

DPO

Het aanstellen van een DPO of functionaris voor gegevensbescherming is volledig nieuw. Sommige ondernemingen zullen een DPO, een soort beheerder voor privacy, moeten aanstellen. Het is een persoon met zowel deskundige als praktische kennis inzake privacy, die de onderneming moet bijstaan bij de interne naleving van de GDPR.

Goed om weten!
De meeste zelfstandige ondernemingen en KMO's zullen geen DPO moeten aanstellen. De aanstelling van een DPO is bedoeld voor ondernemingen voor wie direct marketing of profiling tot hun eigenlijke bedrijfsactiviteiten behoort.

Moet u een DPO aanstellen?

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

O Is uw onderneming een overheidsinstantie?

O Bent u hoofdzakelijk belast met het verwerken van gevoelige gegevens (zie stap 4)?

O Bent u hoofdzakelijk belast met het verwerken van persoonsgegevens die regelmatige en stelselmatige observatie op grote schaal eisen?

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:

O Niet van toepassing

Wat doet zo'n DPO 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
- 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**, bvb een consultant, die deze taak enkele uren per week / maand uitvoert.

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

Meer info vindt u op de website van de Privacy Commissie. Heeft u een DPO nodig, laat u dan bijstaan door een expert om u in orde te stellen met de GDPR.

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

Deze verplichting geldt enkel voor **hoge risicosituaties**.

- Bijvoorbeeld wanneer een nieuwe technologie wordt geïmplementeerd of wanneer een profileringsoperatie een aanzienlijk effect kan teweegbrengen voor de betrokkene.

Goed om weten!
De meeste zelfstandige ondernemingen en KMO's zullen geen DPIA moeten uitvoeren. Vink in dat geval het vakje aan in het grijze kader hieronder.
Een DPIA is (enkel) bedoeld voor ondernemingen die op grote schaal aan direct marketing of profiling doen.

Wat moet er zeker in deze DPIA?

- Beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden.
- Een beoordeling van de noodzaak en proportionaliteit van de verwerking in het licht van de doeleinden.
- Een beoordeling van de risico's voor de rechten en vrijheden van de betrokkenen.
- De maatregelen die overwogen worden om deze risico's te beheersen.

Wanneer de DPIA aangeeft dat het verwerken van de persoonsgegevens een hoog risico inhoudt, moet u advies inwinnen van de Privacy Commissie en de nodige maatregelen nemen om het risico te temmen.

Voor veel zelfstandigen en KMO's zal deze DPIA niet nodig zijn.

Bevindt u zich niet in hogervermelde situatie, vink dan het vakje hieronder aan:

O Niet van toepassing

Op de website van de Privacy Commissie 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
Heeft u personeel?

De GDPR bepaalt ook wat u mag doen met persoonsgegevens van uw medewerker: de loon- en personeelsadministratie, persoonlijke gegevens van sollicitanten of medewerkers, camerabewaking op de werkvloer...

A - Verwerkingsregister

U moet als werkgever in het Register Verwerkingsactiviteiten aangeven wat de rechtsgrond is waarop u zich baseert om bepaalde gegevens te verwerken (zie stap 2). Deze rechtsgrond kan in HR-context bijvoorbeeld zijn:

- de arbeidsovereenkomst tussen u en uw medewerker (in de meeste gevallen)
- een wettelijke verplichting (bijvoorbeeld verwerken van familiale gegevens voor een correcte fiscale behandeling van het loon)
- de behartiging van een gerechtvaardigd belang (bijvoorbeeld bij de verwerking van persoonsgegevens met het oog op netwerk- en informatieveiligheid)
- de uitdrukkelijke toestemming van uw medewerker (bijvoorbeeld voor een foto op de bedrijfswebsite)

B - Documentatie

Om in regel te zijn met de GDPR zal u ook een aantal standaarddocumenten moeten aanpassen:

Sollicitanten laat u best een document ondertekenen waarin ze zich akkoord verklaren met de verwerking van hun persoonsgegevens. Voor uw huidige medewerkers volstaat een aanpassing van de privacy clausule in uw arbeidsreglement.

Heeft u bepaalde afspraken met uw medewerkers rond de verwerking van persoonsgegevens, zoals een policy over camerabewaking of een track-and-tracesysteem? Dan moeten deze ook afgestemd zijn op de nieuwe regels.

C - Geen aangifte meer voor camerabewaking

De aangifteverplichting bij de privacycommissie zoals we die kenden voor de camerabewaking en track-and-trace, is vanaf 25 mei 2018 niet meer nodig. Er blijft wel een aangifteverplichting bestaan bij de politie. Voor deze camera's zal u eveneens een register van beeldverwerkingsactiviteiten moeten bijhouden.

GDPR-Check als u met personeel werkt:

- O De verwerking van gegevens van uw personeel is opgenomen in uw Register Verwerkingsactiviteiten
- O Personeelsdocumenten zijn aangepast door u of uw sociaal secretariaat
- O Uw camerabewaking is aangegeven bij de politie en u houdt een register van beeldverwerkingsactiviteiten bij.

Stap 10
Pas uw privacy policy en contracten aan

Privacy policy

Check of volgende zaken in uw policy staan:

- O De identiteit van de verwerker en de wijze waarop die de gegevens zal aanwenden;
- O De wettelijke grondslag voor gegevensverwerking;
- O De termijnen gedurende dewelke u de informatie zal bijhouden;
- O Of u de gegevens uitwisselt buiten de Europese Unie;
- O 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.
- O De rechten voor de betrokkenen;
- O De technische en organisatorische maatregelen die u zal nemen om compliant te zijn;
- O De doeleinden waarvoor de gegevens zullen worden verwerkt.

Belangrijk is dat u ook hier transparant bent (zie recht op informatie). In ieder geval dient u de privacy policy zo beknopt mogelijk te formuleren in begrijpbare en duidelijke taal.

Beknopt model
Privacy policy

Download één van de UNIZO-modellen

Uitgebreid model
Privacy policy

Contracten

Al uw contracten (met leveranciers, werknemers, verwerkers[1], ...) moeten in overeenstemming zijn met de GDPR.

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.

Check:

- O In uw geschreven contracten zijn de nodige garanties voorzien inzake veiligheid.

1 - 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 en het doorvoeren van de nodige aanpassingen bent u normaal in voldoende mate in overeenstemming met de GDPR. 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/gdpr

UNIZO ONDERNEMERSLIJN
0800 20 750
ondernemerslijn@unizo.be