De GDPR in 10 stappen

Stap 2- Breng in kaart hoe u gegevens verwerkt

De GDPR in 10 Stappen

Stap 2 – Breng in kaart hoe u gegevens verwerkt

Inleiding

In de vorige stap heeft u in kaart gebracht welke gegevens u juist verwerkt. In stap 2 gaan we vervolgens na *hoe* u deze gegevens verwerkt. Onder de GDPR volstaat het immers niet om louter een overzicht te maken van de gegevens die u verwerkt, u moet ook kunnen aantonen dat u deze gegevens op een correcte manier verwerkt. Om na te gaan hoe u gegevens verwerkt, en of dat wel op een correcte manier gebeurt, moeten we 7 vragen overlopen:

1. Zijn de gegevens die u verwerkt proportioneel?
2. Verwerkt u de gegevens enkel voor de doeleinden die u meedeelt?
3. Zijn de gegevens die u verwerkt correct?
4. Op welke juridische basis verwerkt u deze gegevens?
5. Vraagt u op een correcte manier toestemming?
6. Hoe lang bewaart u de gegevens die u verzamelt?
7. Geeft u gegevens door aan derde partijen?

Dit is de langste en misschien ook moeilijkste stap van het Stappenplan. Neem dus de tijd om deze stap zorgvuldig te doorlopen.

Hou er ook rekening mee u er sowieso niet in zal slagen 100% in orde te zijn met de GDPR. Niemand kan dat. Maar eigenlijk verwacht de GDPR dat ook niet. Wat wel verwacht wordt is dat u de keuzes die u in de onderstaande vragen zal maken, kan verantwoorden. Denk er daarom goed over na, en documenteer ook waarom u een bepaalde beslissing neemt.

Vooraleer we aan de vragen beginnen: 'Privacy by design' en 'privacy by default'

Dit zijn twee moeilijke termen om aan te geven dat u zowel bij het bepalen van de manier waarop u gegevens zal verwerken en de middelen die u daarvoor zal inzetten ('privacy by design') als bij de effectieve verwerking zelf ('privacy by default') voldoende maatregelen moet nemen om de beginselen van de GDPR te waarborgen.

Eén van de kernbeginselen van deze twee termen is dat u enkel gegevens mag verwerken die noodzakelijk zijn voor elk specifiek doel van de verwerking, en dan meer bepaald op het vlak van:

- De hoeveelheid gegevens die u verzamelt;
- De mate waarin ze worden verwerkt;
- De termijn voor bewaring van de gegevens;
- De toegankelijkheid van de gegevens.

Wat betekent dat concreet?

- ✓ Als u zelf programma's of toepassingen ontwikkelt waarin persoonsgegevens worden verwerkt, zorg dan dat de standaardinstellingen zo zijn bepaald dat de betrokken gegevens maximaal worden beschermd, door bijvoorbeeld:
  - Niet te veel open velden te voorzien
  - Niet te werken met vooraf aangekruiste vakjes
  - Te voorzien in een verplichting voor de betrokkene om vooraf aan te geven dat hij uw informatieclausules heeft gelezen
- ✓ Als u programma's of toepassingen aankoopt, moet u navragen (én controleren) of de leverancier deze twee principes wel heeft voorzien, en dus of hun producten wel in overeenstemming zijn met de GDPR.

1e vraag: zijn de gegevens die u verwerkt proportioneel?

Zoals al aangegeven, is het doeleinde waarvoor u gegevens verwerkt, cruciaal om te weten wat u juist met de gegevens mag doen. Binnen elk doeleinde mag u immers volgens de GDPR enkel die gegevens verwerken die 'toereikend, ter zake dienend en niet overmatig' zijn.

Het komt er dus op neer dat u enkel gegevens mag verwerken die nodig en relevant zijn voor het doeleinde waarvoor ze verwerkt worden.

Bijvoorbeeld: in het kader van het doeleinde 'klantenbeheer' is het logisch dat u bijvoorbeeld de naam van de klant nodig heeft. Het bijhouden van het rijksregisternummer van de klant lijkt dan weer overmatig te zijn, omdat dat niet echt nodig is om aan klantenbeheer te doen. Op dezelfde manier zijn de detailgegevens van een personeelsevaluatie zijn niet proportioneel in de verwerking die de loonadministratie tot doel heeft. Daar is in beginsel enkel het resultaat van de evaluatie relevant en dus proportioneel omdat deze (wellicht) leidt tot een bonus. Het detail van de evaluatie is enkel relevant en dus proportioneel in de verwerking "personeelsbeheer".

TO DO

Een gegeven dat binnen een doeleinde niet proportioneel is, mag niet langer verwerkt worden binnen dat doeleinde. Indien u de proportionaliteit niet kan verantwoorden binnen een doeleinde, moet u er voor zorgen dat u binnen dat doeleinde dergelijke gegevens niet meer verwerkt.

2e Vraag: verwerkt u de gegevens enkel voor de doeleinden die u meedeelt?

De GDPR legt niet alleen op dat u enkel gegevens mag verwerken die proportioneel zijn binnen een bepaald doeleinde, u mag de gegevens die u binnen dat doeleinde verwerkt bovendien ook *alleen maar* voor dat doeleinde verwerken.

Bijvoorbeeld: de gegevens die u verzamelt voor klantenbeheer, mag u niet gebruiken voor een ander doeleinde (zoals Direct Marketing), zonder de betrokkene daarover vooraf over te informeren of daar toestemming voor te vragen.

U moet met andere woorden, vooraleer u aan de verwerking van een persoonsgegeven begint, aan de betrokkene laten weten voor welk(e) doeleinde(n) u die gegevens verwerkt. U kan later die gegevens niet gaan verwerken voor andere doeleinden dan degene die u op voorhand had aangegeven, tenzij de betrokkene daar toestemming voor geeft.

Dit vraagt, zoals wel vaker bij de GDPR, wat 'gezond verstand'. U zal moeten inschatten welke verwerkingsprocessen binnen een bepaald doeleinde 'redelijk te verwachten vallen'.

Bijvoorbeeld:

- het is niet meer dan logisch dat u binnen het doeleinde 'loonadministratie' de loongegevens van uw medewerkers moet doorgeven aan de RSZ en de FOD Financiën. Dat moet niet beschouwd worden als een afzonderlijk 'doeleinde'.
- als u daarentegen bij het verkrijgen van gegevens van uw klanten, enkel aangeeft dat u die gegevens nodig heeft voor het doeleinde 'klantenbeheer', dan kan u zonder hun toestemming later die gegevens niet verkopen aan derden of hen direct marketing toezenden, omdat dat redelijkerwijze als een ander doeleinde moet worden beschouwd.

In Stap 4 verduidelijken we hoe u op een correcte manier deze informatie aan de betrokkene kan geven.

3e Vraag: zijn de gegevens die u verwerkt correct?

Ga na of u er zeker van bent dat de gegevens die u bijhoudt en verwerkt, wel correct zijn. Als u er aan twijfelt of de gegevens die u bijhoudt nog wel correct zijn, doet u er best aan dat te controleren bij de betrokkene. Let op: u moet niet kunnen garanderen dat alle persoonsgegevens juist zijn. U moet wel kunnen aantonen dat u alle redelijke maatregelen heeft genomen om er voor te zorgen dat de gegevens (zo) juist (mogelijk) zijn.

⇨ Dit is één van de redenen waarom u de laatste weken overstelpt wordt met mails van bedrijven die u vragen om uw gegevens te controleren. U kan er voor kiezen ook zo'n mail te sturen naar uw adressenbestanden, maar eigenlijk geeft u daarmee aan dat u niet zeker bent dat alle gegevens correct zijn. En dat komt natuurlijk ook niet altijd professioneel over… .

4e Vraag: op welke juridische basis verwerkt u deze gegevens?

Het zal u al opgevallen zijn dat, wanneer men over de GDPR spreekt, vaak naar boven komt dat men nu voor alles toestemming moet vragen. Dat klopt echter niet. Wat wel klopt, is dat de GDPR vereist dat u enkel gegevens mag verwerken als u daar een geldige juridische grondslag voor heeft. Toestemming is echter slechts één van die juridische grondslagen. In totaal voorziet de GDPR nog vijf andere mogelijke grondslagen:

1) De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of om vóór de sluiting van de overeenkomst, op verzoek van de betrokkene, maatregelen te nemen;
2) De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting (die op de verwerkingsverantwoordelijke rust) (denk bijvoorbeeld aan de verplichting om te factureren, of loon te betalen aan personeel);

3) De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derden, mits de belangen of grondrechten en fundamentele vrijheden van de betrokkene niet zwaarder (door)wegen;
4) De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor één of meerdere specifieke doeleinden;
5) De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
6) De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of een taak in het kader van uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.

Voor u zijn voornamelijk de eerste vier grondslagen relevant.

U hoeft dus zoals gezegd niet voor alles toestemming te vragen: u moet er gewoon over waken dat u zich kan beroepen op één van de bovenstaande grondslagen en dat u die keuze kan verantwoorden. Zoals u in onderstaand voorbeeld zal merken, zal u slechts zelden echt toestemming moeten vragen.

Voorbeeld

Als we dat bijvoorbeeld toepassen op de doeleinden die we in de 1e stap hebben aangereikt, geeft dat het volgende beeld:

1. Klantenbeheer
   - ☐ Noodzakelijk voor de uitvoering van een overeenkomst
   - ☐ In sommige gevallen: wettelijke verplichting (bijvoorbeeld melding i.k.v. anti-witwaswetgeving)
2. Prospectenbeheer (of Direct Marketing)
   - ☐ Verzamelen van gegevens van prospecten: Gerechtvaardigd belang (vrijheid van ondernemen)
   - ☐ Direct marketing naar klanten en onpersoonlijke mailadressen: Gerechtvaardigd belang (vrijheid van ondernemen)
   - ☐ Direct marketing naar prospecten: toestemming
3. Leveranciersbeheer
   - ☐ Noodzakelijk voor de uitvoering van een overeenkomst
4. Boekhouding
   - ☐ Noodzakelijk voor de uitvoering van een overeenkomst
   - ☐ wettelijke verplichting
5. Communicatie/Public Relations
   - ☐ Gerechtvaardigd belang (vrijheid van ondernemen)
6. Track & trace
   - ☐ Gerechtvaardigd belang (beveiliging van voertuigen, efficiëntie van de werking)
7. personeelsadministratie
   - ☐ Noodzakelijk voor de uitvoering van de arbeidsovereenkomst
   - ☐ wettelijke verplichting (alles wat te maken heeft met uitbetaling van loon en gegevens die doorgegeven moeten worden aan RSZ en FOD Financiën)
   - ☐ Gerechtvaardigd belang (als u bijvoorbeeld controle voert op de online communicatiemiddelen van uw personeel
8. Camerabewaking
   - ☐ Gerechtvaardigd belang (controle op veiligheid)

Let wel op: bijzondere categorieën van persoonsgegevens, zoals gegevens over gezondheid, ras, … mag u niet verwerken, tenzij in zeer uitzonderlijke gevallen. Als u zo'n gegevens zou verwerken, doe dat dan enkel als u daar toestemming voor heeft van de betrokkene.

Heb ik toestemming nodig om commerciële mailings of nieuwsbrieven te versturen?

Eigenlijk wel, maar niet op basis van de GDPR. Om spamming tegen te gaan legt de wetgever op dat een natuurlijke persoon niet commercieel benaderd mag worden via e-mail *zonder zijn voorafgaande, vrije, specifieke en geïnformeerde toestemming.* Anders gezegd: voor direct marketing via mail heeft u inderdaad toestemming nodig. Hier bestaan slechts twee uitzonderingen op:

- ✓ Natuurlijke personen die reeds klant zijn bij u (d.w.z. dat ze een product of dienst hebben afgenomen tegen betaling), mag u wel commerciële boodschappen toezenden per mail zonder dat u daar toestemming voor moet vragen, op voorwaarde dat:
  - U de gegevens rechtstreeks van de klant heeft gekregen
  - de gegevens enkel worden gebruikt voor gelijkaardige producten/diensten die u zelf levert
  - én de klant zich kosteloos kan uitschrijven
- ✓ Elektronische reclame naar onpersoonlijke adressen zoals 'info@...' zijn wel toegelaten, zonder dat u daar toestemming voor moet vragen. Uiteraard moet ook hier een mogelijkheid tot uitschrijven geboden worden.

De vraag is dan natuurlijk hoe lang iemand als ' klant' kan worden beschouwd? Is iemand die 5 jaar geleden iets bij u heeft gekocht nog als 'klant' te aanzien? Helaas is er geen wettelijke regeling voorzien om dit te bepalen. U zal dus zelf een termijn moeten bepalen. Personen die regelmatig in uw winkel komen, zal u zonder meer als klanten mogen beschouwen, waardoor u hen geen toestemming moet vragen om commerciële mails te sturen (als de overige voorwaarden ook voldaan zijn). Personen die slechts één maal iets gekocht hebben, zal u veel sneller moeten schrappen als 'klant' en beschouwen als 'prospect'.

En wat dan met reclame per post of telefoon?

Reclame op papier kan in principe wel nog verstuurd worden, op grond van het gerechtvaardigd belang van vrijheid van ondernemen (op voorwaarde uiteraard dat de betrokkene steeds de mogelijkheid heeft zich hiertegen te verzetten).

Voor telefonische reclame geldt de de 'bel – me – niet – meer' -lijst. Iedereen (zowel een natuurlijke persoon als een rechtspersoon) heeft immers het recht zijn/haar telefoonnummer te laten registreren in die lijst, en van zodra dat gebeurd is, mag u die persoon niet meer telefoneren met een commerciële boodschap. Vooraleer u dus telefonisch prospecteert, moet u die lijst aankopen, en uw bestanden er aan ontdubbelen. Voor meer informatie: https://www.dncm.be/nl/producten-en-tarieven/.

5e Vraag: vraagt u op een correcte manier toestemming?

Volgens de GDPR moet toestemming *vrij, specifiek, geïnformeerd* en *ondubbelzinnig* zijn. Toestemming moet ook steeds een duidelijk *bevestigende handeling* zijn. Gebruik dus geen vooraf aangevinkte vakjes!

Ga na of u de volgende principes hanteert als u om toestemming vraagt:

- ✓ Ik voorzie bij de toestemming een vrijwillige keuze; waarbij de betrokkene uitdrukkelijk kan instemmen *(dit is een zogenaamde '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.

OPGELET: Kinderen

Kinderen vormen een bijzondere categorie van personen. De GDPR legt ten aanzien van kinderen dan ook een aantal specifieke regels op:

- De grondslag 'gerechtvaardigd belang', zal ten aanzien van kinderen in principe niet kunnen worden gebruikt;
- Ten aanzien van kinderen moet informatie op een extra eenvoudige manier worden voorzien;
- Ten aanzien van kinderen vraagt u best toestemming om gegevens te verwerken, evenals aan de ouders.

Desgevallend neemt u de volgende clausule op in uw privacybeleid:

"[VERWERKINGSVERANTWOORDELIJKE] verwerkt in beginsel geen persoonsgegevens van en over minderjarigen. In elk geval verwerkt [VERWERKINGSVERANTWOORDELIJKE] nooit bewust persoonsgegevens van minderjarigen zonder toestemming van hun wettelijke vertegenwoordiger die vereist is om de producten en diensten van [VERWERKINGSVERANTWOORDELIJKE] te gebruiken en om daarna de rechten met betrekking tot de gegevens van de minderjarige uit te oefenen.
Als er toch te goeder trouw persoonsgegevens van minderjarigen zouden verwerkt worden, zal [VERWERKINGSVERANTWOORDELIJKE] deze zo snel mogelijk na kennisname wissen"

6e Vraag: hoe lang bewaart u de gegevens die u verzamelt?

Persoonsgegevens mogen niet eeuwig bewaard worden. Helaas voorziet de GDPR geen wettelijke bewaartermijnen, maar moet u die zelf bepalen. Het gaat evenmin op om voor al uw gegevens één bewaartermijn te voorzien.

U zal dus zelf moeten bepalen hoe lang het volgens u gerechtvaardigd is om een bepaald gegevens bij te houden. Enkele richtlijnen daarbij:

Bewaartermijnen

- **Bewaring gedurende de verwerking**
  Het spreekt voor zich dat u de betrokken persoonsgegevens kan bijhouden zolang u ze nodig heeft voor de verwerking(en) binnen het doeleinde dat u had aangegeven.
  Bijvoorbeeld: Zolang iemand klant is van u, kan u de gegevens in het kader van klantenbeheer bewaren.

- **Bewaring na de verwerking**
  Soms bent u wettelijk verplicht om gegevens ook daarna nog te bewaren. Zo geldt er een wettelijke bewaartermijn van 7 jaar nadat een factuur werd uitgereikt, en een wettelijke bewaartermijn van 5 jaar voor personeelsgegevens.
  Maar ook los van een wettelijke verplichting kan u er baat bij hebben bepaalde gegevens langer te bewaren. Voor verbintenissen uit overeenkomsten kan u bijvoorbeeld (in de meeste gevallen) tot 10 jaar na datum worden aangesproken (de verjaringstermijn voor eventuele rechtsvorderingen door uw medecontractant). U kan dan ook perfect verantwoorden dat u persoonsgegevens die noodzakelijk zijn voor de uitvoering van de overeenkomst, kan bewaren gedurende die verjaringstermijn.

- **Archiveringstermijn**
  Na deze termijnen begint de eigenlijke archiveringstermijn. De GDPR bepaalt dat in dat geval gegevens enkel geanonimiseerd mogen worden bewaard. Bovendien wordt aan elke betrokkene het recht toegekend om de wissing van deze gegevens te vragen zodra ze gearchiveerd worden in deze betekenis.

Die termijnen moeten ook ter kennis worden gebracht van de betrokkenen, in de informatie die hen moet worden verstrekt. Is het niet mogelijk om de bewaringstermijn zelf mee te delen, dan moeten minstens de criteria worden aangegeven die worden gebruikt om die termijn te bepalen. In een aantal privacyverklaringen ziet men nu al de boodschap verschijnen '*Wij bewaren uw persoonsgegevens niet langer dan noodzakelijk voor de beoogde doeleinden van de verwerking*'. Toch doet u er best aan om, waar mogelijk, de bewaartermijn toch concreter te omschrijven, bijvoorbeeld: "*Na het einde van de overeenkomst zullen uw gegevens nog 10 jaar bijgehouden worden (aangezien juridische vorderingen op basis van de overeenkomst tot 10 jaar na datum mogen worden ingediend). "*

TO DO

Het is mogelijk om in een toepassing of programma een termijn op te nemen na verloop van dewelke de gegevens zonder meer worden gewist. Dit vereist vooral dat er voor elk gegeven een duidelijke aanvangstermijn wordt bepaald. Dit moet op een goede manier worden aangepakt omdat het wissen van gegevens die nog nodig of vereist zijn, kan worden aangemerkt als een gegevenslek.
Alternatief kan zijn om periodiek na te gaan of bepaalde gegevens nog wel vereist zijn en ze, indien nodig of aangewezen, te wissen.

Daarnaast moet u een afweging maken om ervoor te zorgen dat de bewaartermijn zoveel mogelijk wordt beperkt (tot wat noodzakelijk is):

- ✓ Zo is het best mogelijk dat om een vordering van een betrokkene te weerleggen, er slechts een beperkt aantal gegevens moeten worden bewaard. In dat geval is in beginsel de bewaring van de andere gegevens niet langer vereist. Dat neemt niet weg dat het in vele gevallen niet evident zal zijn om deze gegevens "uit elkaar te halen".
  In zo'n geval moet het mogelijk zijn om *alle* gegevens gedurende de verjaringstermijn te bewaren, maar dan hanteert u best een passief beheer. Dit houdt in dat de toegang tot die andere gegevens heel beperkt moet worden en blijven.
- ✓ Hou er ook rekening mee dat de bewaartermijn voor 'gevoelige gegevens' hogere eisen stellen, waardoor u er bijvoorbeeld best aan doet de bewaring van dergelijke gegevens bijvoorbeeld extra te beveiligen, bijvoorbeeld door deze gegevens zeker niet op papier te bewaren, maar in een afzonderlijk bestand, indien mogelijk zelfs een afzonderlijke IT-oplossing die gebruik maakt van encyrptie, en bijvoorbeeld slechts voor één persoon toegankelijk is.

7e Vraag: geeft u gegevens door aan derde partijen?

Indien u gegevens doorgeeft aan een derde partij, dan noemt met die derde partij een 'ontvanger' van uw gegevens. Intuïtief zal u misschien aangeven dat u geen gegevens doorgeeft aan dergelijke ontvangers, maar hou er rekening mee dat de term 'ontvangers' veel ruimer is dan u misschien zou denken. Het gaat niet alleen over de vraag of u bijvoorbeeld gegevens verkoopt of doorgeeft aan commerciële partners.

Binnen de groep 'ontvangers' zit immers ook de groep 'verwerkers'. In Stap 1 hebben we gezien dat de verwerker iedere instantie is die gegevens voor u verwerkt. Sociale secretariaten, boekhoudpakketten, IT-leveranciers, … zijn allemaal 'verwerkers', en dus ook 'ontvangers'. Het gaat in al die gevallen om derde partijen die gegevens van u verkrijgen.

TO DO

Breng in kaart aan wie u gegevens doorgeeft. Maak gebruik van algemene categorieën, zoals:

- Commerciële partners
- Overheid
- Verwerkers
- ….

Heeft u al deze vragen geanalyseerd en beantwoord? Dan bent u klaar om naar stap 3 te gaan.

Checklist

- ❑ Ik heb nagekeken welke gegevens binnen elk doeleinde correct zijn en proportioneel, de overige gegevens heb ik verwijderd.
- ❑ Ik heb voor alle gegevens die ik verwerk een geldige juridische grondslag bepaald.
- ❑ Indien ik toestemming moet vragen, heb ik nagekeken of ik die toestemming op een correcte manier vraag.
- ❑ Ik heb voor alle gegevens een passende bewaartermijn vastgelegd.
- ❑ Ik heb in kaart gebracht aan wie ik persoonsgegevens doorgeef.