TECHNISCHE NOTA

Toepassing van de GDPR op de economische beroepsbeoefenaars – verschillende categorieën van gegevens en basisbeginselen

De doelstelling van onderhavige nota bestaat erin om de impact van GDPR voor de economische beroepen te meten aan de hand van concrete voorbeelden.

De economische beroepsbeoefenaars omvatten de boekhouders en fiscalisten (BIBF-leden), de accountants en belastingconsulenten (IAB-leden), alsook de bedrijfsrevisoren (IBR-leden).

Deze beroepsbeoefenaars verwerken en beheren regelmatig bepaalde persoonsgegevens in de zin van de GDPR, zoals de gegevens van hun klanten en leveranciers, de gegevens van de klanten van hun klanten, maar ook de gegevens van hun medewerkers, hun werknemers, hun potentiële klanten, hun zakenrelaties, enz.

Meestal zullen deze gegevens worden verwerkt met behulp van in het kantoor gebruikte boekhoudprogramma's, fiscale applicaties, audittools en documentbeheer- en archiveringssystemen.

Het kantoor dient in zijn hoedanigheid van verwerkingsverantwoordelijke eerst en vooral de verschillende categoriëen van door hem verwerkte gegevens te identificeren.

Verschillende categorieën van gegevens

De GDPR is van toepassing op persoonsgegevens die aan een al dan niet geautomatiseerde verwerking worden onderworpen.

Persoonsgegevens

Het begrip “persoonsgegevens” is ruim gedefinieerd.

Het betreft alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.

> *Bijvoorbeeld : naam, voornaam, beeld (foto’s of video’s aan de hand waarvan de persoon rechtstreeks kan worden geïdentificeerd), nationaal identificatienummer, online identificator, IP adres, vingerafdruk.*

Informatie met betrekking tot rechtspersonen wordt dus niet beoogd.

Gegevensverwerking

De verwerking is ook ruim omschreven en beoogt het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken

door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

In geval van niet-geautomatiseerde verwerking is de GDPR ook van toepassing voor zover de persoonsgegevens in een bestand zijn opgenomen of bestemd zijn om daarin te worden opgenomen.

> *Bijvoorbeeld: klantenbestanden, leveranciersbestanden, interne gebruikerslijst van het kantoor.*

Papieren informatie, voor zover zij gestructureerd is in functie van bepaalde criteria (bvb een alfabetische orde), valt dus ook binnen het toepassingsgebied van de GDPR (dus eventueel: papieren dossier, mappen, fysieke archieven, enz.).

Bijzondere categorieën van persoonsgegevens

Bepaalde categorieën van persoonsgegevens worden beter beschermd:

- persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, genetische gegevens, biometrische gegevens, gegevens over gezondheid, gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid

Verwerking van deze gegevens is in beginsel verboden, maar er zijn uitzonderingen voorzien, meer bepaald op basis van de uitdrukkelijke toestemming, de vitale belangen, de verdediging in rechte, het algemeen belang en de arbeidsgeneeskunde.

> *Kantoren die verantwoordelijk zijn voor de boekhouding of de controle van de jaarrekening van een verzekeringsmaatschappij, een vakvereniging of een politieke partij dienen er in het bijzonder op toe te zien en te waarborgen dat de rechtsgrond voor de gegevensverwerking in kwestie wordt gedocumenteerd.*
>
> *De notulen van een vergadering van een vakbondsafvaardiging of van een ondernemingsraad worden dus geacht gevoeliger van aard te zijn dan de notulen van een raad van bestuur.*
>
> *Evenzo zijn de gegevens uit een patiëntenbestand gevoeliger van aard dan de gegevens uit een klantenbestand van een detailhandelaar.*

- persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten

Deze gegevens mogen alleen worden verwerkt onder toezicht van de overheid.

> *Dit is een aandachtspunt voor boekhouders en commissarissen van advocatenkantoren gespecialiseerd in strafrecht.*

- persoonsgegevens van kinderen

Wanneer de gegevensverwerking berust op toestemming en het kind waarvan de gegevens worden verwerkt jonger is dan 16 jaar, wordt de toestemming verleend door de persoon die de ouderlijke verantwoordelijkheid draagt. Maar 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). In beginsel zal dit niet voorkomen bij de cijferberoepen.

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, bijvoorbeeld in het volgende geval:

> *Een verklaring met betrekking tot een gehandicapt minderjarig kind op grond waarvan een belastingvermindering kan worden genoten,.*

Basisbeginselen

Verantwoordingsplicht

De nieuwe GDPR-regelgeving legt vooral de focus op het bewustmaken van ondernemingen.

De verplichte melding van persoonsgegevensverwerking aan de Commissie voor de bescherming van de persoonlijke levenssfeer is opgegeven. Voortaan moeten ondernemingen er zelf proactief voor zorgen dat hun organisatie aan de GDPR-regels voldoet.

In de praktijk betekent dit dat ondernemingen toelichtingen moeten kunnen geven bij, alsook kunnen aantonen wat zij hebben ondernomen om aan de GDPR-regels te voldoen.

De door ondernemingen voor te leggen **documentatie**, in voorkomend geval via hun IT-contractanten, is bijgevolg essentieel en vormt het uitgangspunt voor de dialoog met de toezichthoudende autoriteit.

Het opstellen van een **gegevensregister** is een dergelijke verplichting.

> *Andere voorbeelden van op te stellen documentatie:*
>
> - *beschrijving van de geïmplementeerde procedures ter beperking van het risico op gegevensverlies;*
> - *beschrijving van de geïmplementeerde procedures voor verlies of diefstal van gegevens;*
> - *in voorkomend geval, het opstellen van een effectbeoordeling;*
> - *in voorkomend geval, het aanstellen van een data protection officer, hierna "DPO", of een soortgelijke functie (cf. infra)*

Rechtmatigheid van de verwerking

De rechtmatigheid van de verwerking is afwisselend gebaseerd op:

-De toestemming

De toestemming moet worden verleend door middel van een ondubbelzinnige actieve handeling.
Het intrekken van de toestemming dient even eenvoudig te zijn als het geven ervan.

Bijvoorbeeld: een schriftelijke verklaring, in voorkomend geval ingediend langs elektronische weg, het selecteren van een vakje op een website.

Vooraf aangevinkte vakjes zijn uitgesloten.

-Een wettelijke verplichting

Bijvoorbeeld in het kader van de antiwitwasverplichtingen: identificatie van klanten, lasthebbers, uiteindelijke begunstigden (ken uw klant-verplichting) en het opslaan van het identiteitsbewijs.
Het is dus niet vereist om toestemming van de klant te vragen voor het verwerken van hem betreffende persoonsgegevens wanneer deze verwerking wettelijk verplicht is.

-Een overeenkomst of precontractuele maatregelen

In een accountants- of auditkantoor is de rechtmatigheid van de verwerking meestal gebaseerd op de uitvoering van een overeenkomst.
Het heeft dus geen zin om systematisch de toestemming van de klant de vragen.
Het opstellen van een opdrachtbrief en/of algemene voorwaarden die dit aspect regelen, is echter van essentieel belang.

-Een taak van algemeen belang of een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen

Bijvoorbeeld de verwerking van persoonsgegevens door het College van toezicht op de bedrijfsrevisoren

-De gerechtvaardigde belangen

Overwegingen 47 tot 49 van de GDPR halen het voorbeeld aan van de verwerking van gegevens van klanten of potentiële klanten ten behoeve van direct marketing.

Fraudevoorkoming wordt ook aangehaald.
Verwerkingsverantwoordelijken die deel uitmaken van een concern kunnen ook een gerechtvaardigd belang hebben bij de doorzending van persoonsgegevens binnen het concern voor interne administratieve doeleinden.
Netwerk- en informatiebeveiliging kan ook een gerechtvaardigd belang vormen.

Deze gerechtvaardigde belangen moeten evenwel tegen de mogelijke schending van de rechten en vrijheden van de betrokkene worden afgewogen (afweging van de betrokken belangen). De aard van de verwerkte gegevens en de redelijke verwachtingen van de betrokkenen dienen in aanmerking te worden genomen.

Behoorlijkheids- en transparantiebeginsel

De rechten van de betrokkene krijgen een belangrijke rol toebedeeld in de nieuwe regelgeving.

Persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt.

Recht van inzage van de betrokkene houdt in dat de betrokkene het recht heeft om van de verwerkingsverantwoordelijke uitsluitsel te verkrijgen over het al dan niet verwerken van hem betreffende persoonsgegevens. Wanneer dat het geval is, moet de betrokkene inzage verkrijgen van die persoonsgegevens en van informatie die meer bepaald betrekking heeft op:

- de verwerkingsdoeleinden;
- de betrokken categorieën van persoonsgegevens;
- de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen (...).

De verwerkingsverantwoordelijke beschikt over een termijn van één maand om te reageren op het verzoek om informatie van de betrokkene (eventueel verlengd met twee maanden). Elke weigering om het verzoek in te willigen dient met redenen te worden omkleed.

Verder dient ook te worden vermeld dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken om rectificatie of wissing (recht op vergetelheid) van de persoonsgegevens.

Het kantoor dient dus de bestaande procedures te beoordelen teneinde meer bepaald na te gaan of de systemen de betrokkene toelaten om zijn rechten uit te oefenen.

Verder dient de geheimhoudingsverklaring van het kantoor te worden beoordeeld en, in voorkomend geval, aangepast, zodat deze de door de GDPR vereiste informatie bevat, zoals de rechtmatige grondslag voor de gegevensverwerking en de opslagperiodes.

Het kantoor dient zich er ook van te vergewissen dat de opgeslagen gegevens juist zijn en worden geactualiseerd. Alle maatregelen moeten worden getroffen om de onjuiste gegevens onverwijld te wissen of te rectificeren.

OVER PROFILERING

De GDPR omschrijft profilering als elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Krachtens de antiwitwasbepalingen moeten alle kantoren een risicoprofiel opstellen van al hun klanten. De kantoren mogen uiteraard geen informatie hieromtrent verstrekken aan hun klanten.

Relevantie- en minimaliseringsbeginsel

Verwerking van persoonsgegevens moet altijd worden beperkt tot hetgeen strikt noodzakelijk is.

Gegevens mogen niet langer worden bijgehouden dan noodzakelijk is voor de beoogde doeleinden van de verwerking.

In het kader van een opdracht verzamelt een kantoor diverse persoonsgegevens. Enkel de gegevens die nodig zijn voor het uitvoeren van de opdracht dienen te worden vastgelegd. Verder dient het kantoor te beschikken over een procedure om ervoor te zorgen dat de vastgelegde gegevens niet langer dan nodig worden bijgehouden.

De kantoren dienen de persoonsgegevens te identificeren die werden bijgehouden op een andere grond dan een wettelijke verplichting en die na het verstrijken van de bewaartermijn absoluut moeten worden vernietigd.

Het is niet eenvoudig om gegevens die uit dien hoofde werden bijgehouden, af te zonderen van andere gegevens die werden bijgehouden op grond van een wettelijke verplichting en waarvan de bewaringstermijn langer kan zijn. Dit houdt dat de archieven, met inbegrip van de elektronische archieven, op adequate wijze worden beheerd.

In bepaalde gevallen kan het gerechtvaardigd zijn om de persoonlijke gegevens langer bij te houden dan vereist op grond van een specifieke wetgeving, bijvoorbeeld om zich, in voorkomende geval, doeltreffend in rechte te kunnen verdedigen.