De heer Mathieu Michel
Staatssecretaris
Karmelietenstraat 15
1000 Brussel

Sint-Niklaas, 30 april 2021

Geachte heer Michel,

Beltug is de vereniging van CIOs en hun collega's die nauw betrokken zijn bij de digitalisering binnen bedrijven en overheidsinstelingen. Binnen onze vereniging, van bijna 490 organisaties, is er een Privacy Council actief, waarin meer dan 60 privacyspecialisten van uiteenlopende sectoren, ervaringen uitwisselen. Het gaat daarbij voornamelijk om DPOs en mensen die binnen hun bedrijf of instelling zeer nauw betrokken zijn met het naleven van de GDPR en de Belgische wet.

Onze inbreng is gebaseerd op hun praktijkervaring.

1. De wet van 30 juli 2018 is moeilijk leesbaar en de afwijkingen van de GDPR-tekst zijn niet steeds even duidelijk. Een overzicht van de Belgische afwijkingen en/of toevoegingen, met een referentie naar de bijhorende artikels van de GDPR-tekst is erg welkom.

2. Naar een sterkere en pragmatische GBA.

   Algemeen kan men stellen dat de regelgeving rond privacy tot een spanningsveld heeft geleid tussen de vele mogelijke interpretaties enerzijds, en de concrete implementatie anderzijds.

   De Belgische GBA is een kleine organisatie met beperkte middelen. Dit leidt tot een aantal problemen in de praktijk. Zo is de antwoordtijd van de GBA onvoorspelbaar en vaak te lang. Bedrijven die de GBA inschakelen zijn net de bedrijven die de GDPR ter harte nemen. Het is erg vervelend dat vragen te laat of zelfs niet worden beantwoord. Ondertussen tasten organisaties in het duister en lopen ze risico's op klachten, onderzoeken of boetes.

   Het zou goed zijn als de GBA met bedrijven in discussie zou gaan om op basis van de vragen en moeilijkheden in de praktijk richtsnoeren op te maken. Er is echt nood aan concrete aanbevelingen. Dit zou kunnen leiden tot belangrijke schaalvoordelen en grotere zekerheid, omdat niet elk bedrijf zelf de teksten moet interpreteren.

   Andere lidstaten hebben deze mogelijkheden ingebouwd in hun werking. Het is daarom belangrijk om initiatieven zoals het wetsvoorstel van 4 maart 2021 *"tot wijziging van de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit en tot wijziging van de wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, wat de voorafgaande beslissingen betreft"* te ondersteunen omdat dit een stap in die richting is.

   En waarom zelfs niet te denken aan een *Privacy ruling*, zodat een organisatie van de GBA een bindend advies kan krijgen?

   De mogelijkheid van *regulatory sandboxes* wordt best overwogen.

Het zou ook goed zijn om sturing te krijgen rond bepaalde software leveranciers die door veel bedrijven gebruikt worden, en waar de GDPR compliance een probleem stelt.

Een vereenvoudiging van de structuur van de GBA is welkom, met verduidelijking van de beslissingsbevoegdheden.

3. VTC en GBA zijn twee aparte organen voor de controle en de handhaving van de vereisten rond gegevensbescherming. Beide organen hebben verschillende verantwoordelijkheden. Het is echter niet steeds duidelijk of beide organen dezelfde adviezen ondersteunen. Het meest sprekende, en zeer belangrijk advies van de VTC is het advies en waarschuwing m.b.t. dataplatformen in publieke cloud. Al is advies gericht naar de Vlaamse Overheid, het heeft tot veel ongerustheid geleid m.b.t. het gebruik van buitenlandse cloud platformen, ook bij bedrijven.

4. Rechtszekerheid : onder meer het Europees Hof van Justitie te Luxemburg velt arresten m.b.t. gegevensbescherming. De impact van deze arresten kan verregaand zijn. Zo heeft het Schrems II arrest van 16 juli 2020 geleid tot een vacuüm. Naast de informatie gepubliceerd op de website, zou de GBA in deze context een belangrijkere rol kunnen spelen, door aan te geven hoe bedrijven de transitieperiode - tot er een opnieuw een internationale oplossing is - kunnen overbruggen.

5. Eén van de meest voorkomende discussies is de toewijzing van de rollen verwerkingsverantwoordelijke / verwerker. Het zou bijzonder behulpzaam zijn, mocht de GBA een lijst opmaken van de meest voorkomende gevallen, uiteraard omschreven met de correcte bepalingen om discussies te vermijden. Belangrijk om weten is dat steeds meer organisaties de toewijzing 'verwerker' afwijzen en 'verwerkingsverantwoordelijke' als rol opnemen wat niet de bedoeling is.

6. Een algemene feedback van de meeste belangrijke breaches en de maatregelen die moeten genomen worden zou nuttig zijn.

7. Uit onze dagelijkse contacten blijkt duidelijk hoeveel vragen er zijn rond privacy. Dit zal alleen maar belangrijker worden.

   Met concrete adviezen kan men er voor zorgen dat niet elke organisatie een oplossing moet zoeken voor gelijkaardige problemen.

   Alle bedrijven zitten in de digitale transformatie, en dataverwerking staat hierbij centraal.

   Er is nood aan advies vanuit de GBA m.b.t. de integratie van gegevensbescherming met

   - Informatieveiligheid (zo is integratie van bepaalde adviezen van het Cyber for Security Centre Belgium welkom).
   - Data management (AI & Analytics)

   De GBA kan een bondgenoot zijn van de bedrijven en overheidsinstellingen. Er is een belangrijke rol weggelegd, die veel verder gaat dan het uischrijven van boetes en het geven van adviezen op de wetgeving.

   Op deze manier zou de GBA de economie kunnen ondersteunen door op een aantal prangende vragen bij de digitalisering een concreet antwoord te geven.

Bijkomende suggesties

- Duidelijk opnemen van een lijst van uitzonderingen onder lokaal recht per bepaling in de AVG waarin deze mogelijkheid wordt voorzien. In het bijzonder zou voor artikel 9.2 (naar het voorbeeld van de UK law) een extensieve lijst van uitzonderingen kunnen worden opgenomen (vb. Covid issues, biometrische gegevens voor toegangscontrole, etc.). Daarnaast wordt idealiter ook een lijst van uitzonderingen op de rechten van de betrokkenen opgenomen (zie eveneens UK law als voorbeeld).
- In allerlei wetgeving uitdrukkelijk aangeven dat een bepaalde opdracht een 'taak is van algemeen belang' om rechtszekerheid over de toepasselijke rechtsgrond te bieden.

  Ter illustratie

  Publieke overheidsbedrijven behoren tot de publieke sector, maar zijn geen publieke sector in strikte zin. Bepaalde reglementeringen zijn enkel van toepassing op de publieke sector, maar dit is niet altijd even duidelijk. In bepaalde gevallen worden er uitzonderingen in de kaderwet zelf voorzien. Zo zijn publieke overheidsbedrijven bv. wel onderhevig aan administratieve boetes (deze uitzondering is bv. expliciet voorzien in art. 221 §2 Belgische kaderwet).

  Het zou verduidelijkt kunnen worden dat publieke overheidsbedrijven wel degelijk op het gerechtvaardigd belang als grondslag beroep kunnen doen voor zaken die niet strikt tot de uitoefening van taken van algemeen belang behoren.

- In het artikel 20 § 1 van de Wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens van 30 juli 2018 wordt bepaald dat de federale overheid de doorgifte aan enig andere overheid of privéorgaan van persoonsgegevens voor elk type van verwerking op basis van artikel 6.1.c) en e), van de Algemene Verordening Gegevensbescherming formaliseert aan de hand van een protocol dat tot stand komt tussen de initiële verwerkingsverantwoordelijke en de verwerkingsverantwoordelijke ontvanger van de gegevens, tenzij anders bepaald in bijzondere wetten, en dit in uitvoering van artikel 6.2. van de Algemene Verordening Gegevensbescherming.

  Art. 20 § 2.: Het protocol wordt afgesloten na de respectievelijke adviezen van de functionaris voor gegevensbescherming van de federale overheid die houder is van de persoonsgegevens en van de bestemmeling. Deze adviezen worden toegevoegd aan het protocol. Wanneer ten minste een van deze adviezen niet gevolgd wordt door de verwerkingsverantwoordelijken vermeldt het protocol, in zijn inleidende bepalingen, de reden of redenen volgens dewelke het advies of de adviezen niet werden gevolgd.

  In de praktijk werkt dit duidelijk anders, en wordt een protocolontwerp reeds opgesteld waarover dan het advies van een DPO gevraagd wordt. Dit advies wordt dan weer verwerkt in het protocol, waarover opnieuw advies gevraagd wordt. Het is geen werkbare procedure om dan een advies te geven die aan het protocol wordt toegevoegd en openbaar wordt gemaakt (zie §3).

  Art. 20 §3: Het protocol wordt openbaar gemaakt op de website van de betrokken verwerkingsverantwoordelijken.

  Voorstel

  - De adviezen zouden eerder moeten beschouwd worden als intern aan de organisatie.

- Het zou minstens aangewezen zijn dat de federale overheid gebruik maakt van specifieke templates die een uitvoering geven aan dit artikel.

- Het Belgisch regime voor onderzoek, historische en statische doeleinden wordt best herwerkt (Titel 4 Gegevensbeschermingswet (GBW)).
- Consolideren van privacy-bepalingen in allerlei wetgeving (vaak nog met verwijzing naar de Privacywet uit 1992 / verwijzing naar de Commissie voor de bescherming van de persoonlijke levenssfeer / sectorale comités). Het mechanisme uit artikel 253 GBW kan aanleiding tot verwarring geven.
- Het creëren van een duidelijkere opdeling van de Privacywet (duidelijk onderscheid tussen algemeen deel en bijzondere delen).
- In de mate dat de Wet tot oprichting van de gegevensbeschermingsautoriteit eveneens zou worden herzien, wensen wij nog aan te merken dat de basisprincipes van de rechten van verdediging onvoldoende worden verankerd (cf. samenwerkingsakkoord tussen GBA en DNS Belgium, geen systematische hoorplicht,…). Bovendien zijn er weinig procedure termijnen in de wet voorzien om het verloop van de procedure adequaat te kunnen bepalen.
- Gedragscodes: een vereenvoudiging van de regels is aangewezen. De gedragscode is een instrument dat best verder wordt ontwikkeld. Een groter gebruik kan de GBA ontlasten van een bepaald aantal vragen, zaken en geschillen.
- Het zou goed zijn als de GBA eraan gehouden wordt om de betrokkenen te informeren wanneer een dossier wordt afgesloten.

- De Privacywet bevat een Ondertitel 3 met betrekking tot verwerken van veiligheidsmachtigingen en dergelijke (art. 103 – 137). Art. 124 bepaalt dat een Data Protection Officer altijd over een veiligheidsmachtiging "zeer geheim" moet beschikken. Het heeft geen zin dat een DPO een veiligheidsmachtiging zou moeten hebben die hoger is dan het niveau van de geclassificeerde informatie van de organisatie waar hij voor werkt. Indien de organisatie enkel "geheime" informatie verwerkt zou dat ook moeten volstaan voor de veiligheidsmachtiging van de DPO.

Vanzelfsprekend zijn wij graag ter uwer beschikking voor meer informatie,
Met vriendelijke groeten,

Danielle Jacobs
CEO Beltug