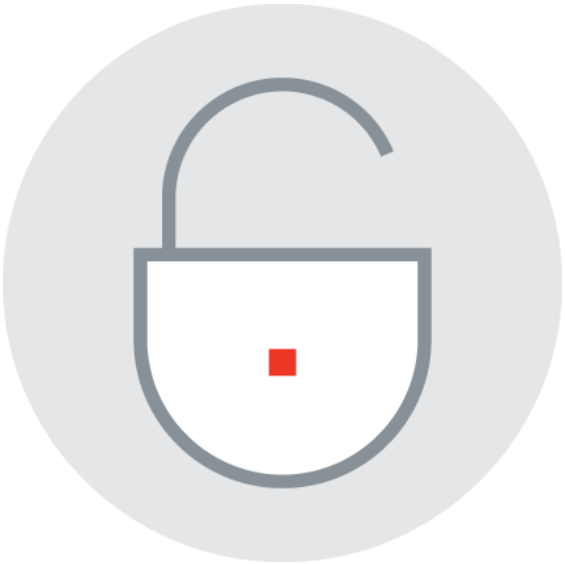
September 2018

Ius Laboris Belgium Global HR Lawyers
Claeys & Engels

Newsletter:
De Belgische Gegevensbeschermingswet treedt vandaag in werking

Inhoudstafel



Beste lezer,

De Europese Algemene Verordening Gegevensbescherming - beter gekend onder de afkortingen “AVG” of “GDPR” - is op 25 mei 2018 van toepassing geworden.

Ondernemingen zouden intussen het nodige moeten hebben gedaan om hun verwerkingsactiviteiten in lijn te brengen met de GDPR en op een juiste manier te omkaderen.

De krachtlijnen van de GDPR werden reeds besproken in onze Newsletter van 4 mei 2016 . Ook op onze website www.gdprbelgium.be hebben wij heel wat informatie over de GDPR gebundeld.

Hoewel de GDPR een harmonisatie van de regels inzake gegevensbescherming binnen Europa beoogt, wordt tevens een opening gelaten voor lidstaten om eigen accenten te leggen en specifieke voorschriften te voorzien in de nationale wetgeving, bijvoorbeeld op het vlak van arbeidsrecht. Uiteraard moet dit gebeuren binnen de grenzen van de GDPR.

Vandaag werd de langverwachte Belgische “wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens” (hierna: Gegevensbeschermingswet) gepubliceerd in het Belgisch Staatsblad. Deze wet heft de vorige Gegevensbeschermingswet van 8 december 1992 op, en treedt vandaag in werking.

Wij geven jullie hierbij graag een samenvatting van de belangrijkste regels die een impact hebben op vrijwel alle ondernemingen.

Wij wensen u veel leesplezier!

1 Toepassingsgebied

De Belgische Gegevensbeschermingswet is in eerste instantie van toepassing op verwerkingen in het kader van de activiteiten van een Belgische vestiging van een verwerker of verwerkingsverantwoordelijke, ongeacht of de verwerking zelf al dan niet in België plaatsvindt.

Een uitzondering hierop geldt voor een Belgische verwerker die werkt in opdracht van een verwerkingsverantwoordelijke uit een andere EU lidstaat en de verwerking ook plaatsvindt in deze andere EU lidstaat. In dat geval is het recht van deze andere EU lidstaat van toepassing.

De Belgische Gegevensbeschermingswet kan echter ook van toepassing zijn op niet-Europese ondernemingen die geen vestiging hebben in België. Dat is het geval indien een onderneming:

- goederen of diensten aanbiedt aan personen in België, ongeacht of hiervoor al dan niet betaald moet worden;
- het gedrag van personen in België observeert, door bijv. *online profiling*.

2 Gevoelige persoonsgegevens

Op basis van de GDPR genieten een aantal bijzondere categorieën van persoonsgegevens van een specifiek regime gelet op hun gevoelig karakter: genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid, gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. Ook voor gegevens m.b.t. het strafrechtelijk verleden van iemand, in België aantoonbaar door het uittreksel uit het strafregister, geldt een specifiek regime.

2.1 Principieel verbod op verwerking

De verwerking van dergelijke gevoelige gegevens is in principe verboden, tenzij de onderneming zich hiervoor op een uitzondering kan beroepen.

Een van de uitzonderingen is de noodzakelijkheid omwille van redenen van zwaarwegend algemeen belang. De Belgische Gegevensbeschermingswet bepaalt dat verenigingen en stichtingen waarvoor de verwerking van gevoelige gegevens noodzakelijk is voor de verwezenlijking van hun statutair doel, zich onder bepaalde voorwaarden op deze uitzondering kunnen beroepen.

De andere uitzonderingen van de GDPR, bijvoorbeeld wanneer de verwerking noodzakelijk is om te voldoen aan arbeidsrechtelijke verplichtingen, blijven hier uiteraard naast bestaan.

2.2 Genetische, biometrische en gezondheidsgegevens

De verwerking van dergelijke gegevens is verboden, tenzij een onderneming zich op een van de uitzonderingen kan beroepen. Zo is de verwerking van dergelijke gegevens wel mogelijk wanneer iemand daar zijn/haar toestemming voor geeft. In het kader van een arbeidsrelatie riskeert toestemming echter ongeldig te zijn omdat het vrije karakter ervan betwist kan worden.

Op het vlak van het arbeidsrecht voorziet de GDPR echter wel de mogelijkheid voor lidstaten om bijkomende uitzonderingen voor het verwerken van dergelijke gegevens te bepalen. Sommige landen hebben van deze mogelijkheid gebruik gemaakt om onder bepaalde voorwaarden toegangscontrole via bijv. een vingerafdruk of irisscan mogelijk te maken. In de Belgische wetgeving is dergelijke uitzondering echter niet voorzien, en ook de Gegevensbeschermingswet maakt geen

gebruik van deze mogelijkheid. Voor werkgevers zal het bijgevolg moeilijk blijven om biometrische authenticatiesystemen voor toegangscontroles en tijdsregistratie te gebruiken, ermee rekening houdend dat de situatie geval per geval beoordeeld moet worden.

Voor de verwerking van genetische, biometrische en gezondheidsgegevens bevestigt de nieuwe Gegevensbeschermingswet wel de bijkomende voorwaarden die reeds bestonden op basis van de opgeheven reglementering. Er geldt met name een verplichting om een lijst op te stellen met categorieën van personen die toegang hebben tot deze gegevens en een omschrijving van hun rol in het kader van deze verwerking. Deze lijst moet kunnen worden voorgelegd aan de Gegevensbeschermingsautoriteit (hierna: "GBA") indien deze hierom verzoekt. De personen die toegang hebben moeten verder gebonden zijn door een wettelijke of contractuele vertrouwelijkheidsverplichting.

2.3 Strafrechtelijke gegevens

De verwerking van gegevens over het strafrechtelijk verleden van personen, zoals bijv. een uittreksel uit het strafregister, is in principe verboden.

De Gegevensbeschermingswet bepaalt hierop nu enkele uitzonderingen. Zo is een verwerking van strafrechtelijke gegevens onder meer mogelijk:

- wanneer dit noodzakelijk is voor het beheer van eigen geschillen;
- door advocaten of andere juridische raadgevers in zoverre de verdediging van de belangen van hun cliënten dit vereist;
- voor redenen van zwaarwegend algemeen belang voor het vervullen van taken van algemeen belang die door een wet, decreet, ordonnantie of Europees recht zijn vastgesteld;
- indien de betrokken persoon deze gegevens kennelijk op eigen initiatief openbaar heeft gemaakt voor een of meer welbepaalde doeleinden;
- indien de betrokken persoon hiervoor toestemming geeft. Deze uitzondering zal o.i. echter niet gebruikt kunnen worden door werkgevers. Omwille van het ondergeschikt verband in een arbeidsrelatie kan de toestemming immers als niet-vrij en bijgevolg als ongeldig worden beschouwd. Deze nieuwe uitzondering biedt echter wel opportuniteiten in andere situaties dan de arbeidsrelatie. Je zal er dan wel voor moeten zorgen dat de toestemming voldoet aan de strikte voorwaarden van de GDPR: deze moet vrij, specifiek, op informatie berustend en ondubbelzinnig zijn en in een duidelijke en begrijpbare taal worden geschreven.

Gelet op het verbod en de strikte uitzonderingen zullen werkgevers uit de privésector in principe dus geen uittreksel uit het strafregister van werknemers of sollicitanten kunnen bewaren, tenzij één van voormelde uitzonderingen van toepassing is.

We herinneren eraan dat de GBA in het verleden heeft aangegeven dat je in de andere gevallen aan een (kandidaat-)werknemer wel mag vragen om een uittreksel uit het strafregister vrijwillig te tonen, maar dat je hiervan echter geen kopie mag nemen, dit bewaren of er enige nota van nemen.

3 Aanbod van diensten van de informatiemaatschappij aan kinderen

Volgens de GDPR moeten jongeren tot 16 jaar de toestemming krijgen van hun ouders om toegang te krijgen tot "diensten van de informatiemaatschappij" zoals sociale media, websites, apps, ... De verantwoordelijkheid om dat na te gaan ligt bij de aanbieders van deze diensten. Lidstaten kunnen de leeftijdsgrens echter verlagen tot minimum 13 jaar, en van deze mogelijkheid heeft België gebruik gemaakt.

Op basis van de Belgische Gegevensbeschermingswet zullen jongeren vanaf 13 jaar bijgevolg zelf hun toestemming moeten geven voor een verwerking van hun persoonsgegevens wanneer zij gebruik maken van sociale media, website, apps, ...

De GBA had positief advies gegeven over de verlaging van deze leeftijd naar 13 jaar aangezien deze leeftijd beter aansluit bij de dagdagelijkse praktijk waarbij heel wat jongeren zich reeds vanaf jonge leeftijd online begeven.

4 Uitzonderingsregime voor verwerkingen voor historische, statistische of wetenschappelijke doeleinden

Om wetenschappelijk en historisch onderzoek en het produceren van statistieken te faciliteren, kunnen lidstaten in hun nationale wetgeving afwijkingen voorzien op de volgende rechten: toegang, rectificatie, beperking en bezwaar. Het afwijkingsregime kan echter enkel worden toegepast voor zover de bovenstaande rechten de verwezenlijking van de specifieke kennisdoeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren, en dergelijke afwijkingen noodzakelijk zijn om die doeleinden te bereiken.

De bovenstaande verwerkingen voor kennisdoeleinden moeten ruim worden opgevat. Het gaat niet enkel om onderzoeksactiviteiten in een academisch kader, maar het kan ook *research & development* activiteiten van bedrijven omvatten, hoe klein ook. Een voorbeeld aangehaald door de Gegevensbeschermingsautoriteit in zijn advies over het voorontwerp van Gegevensbeschermingswet is een bedrijf dat een groep consumenten uitnodigt om te peilen of een nieuw ontwikkelde verpakking gebruiksvriendelijker is dan de huidige verpakking. Volgens de Gegevensbeschermingsautoriteit is de impact dus niet beperkt tot universiteiten of welbepaalde innovatie-gerichte bedrijven, maar worden tevens kleinschalige onderzoeksactiviteiten geviseerd. Uit de parlementaire voorbereiding van de wet blijkt echter dat niet alle leden van de regering het met dit standpunt eens zijn, en dat volgens hen enkel wetenschappelijk onderzoek in de strikte zin onder dit uitzonderingsregime zou vallen. Volgens dit standpunt zou het uitzonderingsregime enkel van toepassing zijn wanneer het wetenschappelijk onderzoek een maatschappelijk belang - en niet louter een privébelang - dient. De precieze draagwijdte van dit uitzonderingsregime zal bijgevolg nog verder uitgeklaard moeten worden.

Om het uitzonderingsregime uit de GDPR te kunnen toepassen bepaalt de Gegevensbeschermingswet de onderstaande waarborgen, die bijkomende verplichtingen met zich meebrengen voor alle bedrijven die verwerkingen voor kennisdoeleinden verrichten zoals hierboven toegelicht.

4.1 Anonimisering of versleuteling

Volgens de GDPR kan versleuteling een gepaste maatregel zijn om persoonsgegevens te beschermen, en moet anonimisering worden toegepast waar mogelijk.

In lijn met de vroegere reglementering, gaat de Gegevensbeschermingswet een stapje verder en voert een soort cascadesysteem in:

- in principe moeten gegevens geanonimiseerd worden zodat de betrokken personen niet meer geïdentificeerd kunnen worden;
- wanneer dat niet mogelijk is, zullen gegevens versleuteld of gecodeerd moeten worden (zogenaamde “pseudonimisering”). Op die manier kunnen gegevens niet meer aan een bepaalde persoon worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt. Deze aanvullende gegevens moet afzonderlijk bewaard en op afdoende wijze beveiligd worden;

- enkel wanneer ook versleuteling niet mogelijk is, kunnen niet-versleutelde gegevens gebruik worden. Niet-versleutelde gegevens mogen echter in principe niet verspreid of meegedeeld worden aan derden.

4.2 Uitgebreider register van de verwerkingsactiviteiten

Ondernemingen die persoonsgegevens verwerken voor kennisdoeleinden, dienen de volgende elementen toe te voegen aan het register van de verwerkingsactiviteiten:

- de verantwoording van het gebruik van de al dan niet versleutelde gegevens;
- waarom de uitoefening van het recht op toegang, rectificatie, beperking en/of bezwaar door de betrokkene de verwezenlijking van de kennisdoeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren;
- in geval van verwerking van “gevoelige gegevens”, de gegevens-beschermingseffectbeoordeling (indien van toepassing).

4.3 Uitgebreidere informatieverplichting

In het kader van de GDPR moet de verwerkingsverantwoordelijke heel wat informatie verstrekken aan de personen wiens gegevens hij verwerkt. Ondernemingen die gegevens verwerken voor kennisdoeleinden zullen nog over twee bijkomende elementen moeten informeren indien zij de gegevens verzamelen rechtstreeks bij de betrokkene:

- het feit dat de gegevens al dan niet worden geanonimiseerd;
- waarom de uitoefening van het recht op toegang, rectificatie, beperking en/of bezwaar door de betrokkene de verwezenlijking van de kennisdoeleinden onmogelijk dreigen te maken of ernstig dreigen te belemmeren.

Indien de gegevens niet rechtstreeks bij de betrokkene worden verzameld, zal een overeenkomst moeten worden gesloten met de verantwoordelijke voor de oorspronkelijke verwerking (van wie de gegevens verkregen worden) of, in geval van vrijstelling van het afsluiten van een overeenkomst, een kennisgeving aan deze laatste moeten gebeuren. Deze documenten moeten tevens bij het register van de verwerkingsactiviteiten gevoegd worden.

5 Functionaris voor gegevensbescherming: bijkomende verplichtingen

Op basis van de GDPR zijn sommige ondernemingen, zoals publieke overheden of ondernemingen waarvan de hoofdactiviteit bestaat in een grootschalige verwerking van gevoelige gegevens (bijv. ziekenhuizen) of in een stelselmatige observatie op grote schaal van personen (bijv. verzekeringsondernemingen) verplicht om een zogenaamde “functionaris voor gegevensbescherming” (DPO of *data protection officer*) aan te stellen.

De Gegevensbeschermingswet voegt hier nog twee mogelijke gevallen van verplichte aanstelling van een DPO aan toe:

- een onderneming of instelling die verwerkingen verricht voor wetenschappelijk of historisch onderzoek of voor statistische doeleinden;
- een privébedrijf dat persoonsgegevens verwerkt voor rekening van een federale overheid of waaraan een federale overheid persoonsgegevens doorgeeft.

In lijn met de risicogebaseerde benadering van de GDPR, zal in de twee bovenstaande gevallen enkel een DPO moeten worden aangesteld indien de verwerking van deze gegevens een “hoog risico” kan inhouden.

Voor de betekenis van “hoog risico” wordt verwezen naar de verplichting tot het uitvoeren van een zogenaamde

"gegevensbeschermingseffectbeoordeling" (GEB, ook wel DPIA genoemd naar de Engelse benaming: *data protection impact assessment*) voor risicovolle verwerkingsactiviteiten.

De GDPR geeft geen definitie van dit begrip "hoog risico". De *European Data Protection Board* of EDPB (voorheen: Artikel 29-werkgroep), het overkoepelend Europees orgaan van toezichthoudende autoriteiten, en de Belgische GBA hebben dit begrip in hun adviezen verduidelijkt en een aantal situaties opgelijst waarin een GEB steeds vereist is, zoals ingeval van grootschalige verwerking van biometrische gegevens, bijv. in het kader van genetisch onderzoek.

Voor meer informatie over de verplichting tot het uitvoeren van een GEB: zie onze Newsflash van 28 maart 2018.

6 Rechtsmiddelen

6.1 Overzicht

Personen die menen het slachtoffer te zijn van een inbreuk op de wetgeving inzake gegevensbescherming of zich belemmerd voelen in de uitoefening van hun rechten, hebben de volgende actiemogelijkheden:

- een klacht bij de bevoegde GBA (niet noodzakelijk de Belgische);
- een vordering tot staking bij de rechtbank om de inbreuk te laten ophouden;
- een schadeclaim bij de rechtbank.

De Belgische Gegevensbeschermingswet bepaalt de mogelijkheid om zich hierbij te laten vertegenwoordigen door een organisatie of vereniging die actief is op het gebied van gegevensbescherming. Deze organisatie of vereniging kan dan een klacht neerleggen of naar de rechtbank stappen in naam van de betrokken natuurlijke perso(o)n(en). Deze organisatie of vereniging moet hiertoe echter de opdracht krijgen en kan niet op eigen initiatief een zaak aanhangig maken bij de GBA of de rechtbank.

6.2 Vordering tot staking

Wanneer een persoon of de GBA een inbreuk op de wetgeving inzake gegevensbescherming wil laten ophouden of de uitoefening van zijn rechten wil afdwingen, kan deze een vordering tot staking indienen bij de voorzitter van de rechtbank van eerste aanleg, zitting houdende zoals in kort geding. Het gaat bijgevolg om een procedure met verkorte termijnen om snelle actie mogelijk te maken.

De voorzitter van de rechtbank van eerste aanleg kan in een "stakingsbevel" de volgende maatregelen opleggen:

- een termijn toestaan om een einde te maken aan een inbreuk of om een verzoek tot uitoefening van rechten in te willigen;
- openbaarmaking: aanplakking van de beslissing (of een samenvatting ervan) binnen of buiten de onderneming, en/of de publicatie ervan in kranten;
- indien onjuiste, onvolledige of niet ter zake dienende persoonsgegevens of persoonsgegevens waarvan de bewaring verboden is, aan derden werden meegedeeld, kan de verwerker of verwerkingsverantwoordelijke worden verplicht om aan deze derde(n) kennis te geven van de beperking, rectificatie of verwijdering van die persoonsgegevens.

Indien dwingende redenen bestaan om te vrezen dat bewijselementen ter ondersteuning van een stakingsvordering zouden verdwijnen of ontoegankelijk gemaakt zouden worden, kan de eiser via een eenzijdig verzoekschrift aan de voorzitter van de rechtbank van eerste aanleg vragen om maatregelen te gelasten om dergelijke verdwijning of ontoegankelijkheid te voorkomen.

7 Sancties

De GDPR vereist een systeem van sancties dat doeltreffend, evenredig en afschrikkend is.

7.1 Administratieve sancties

Bedrijven die de regels aan hun laars lappen kunnen door de GBA zwaar beboet worden met administratieve geldboetes die kunnen oplopen tot 20 miljoen euro of 4% van de jaarlijkse wereldwijde omzet van een onderneming.

De GBA kan echter ook andere corrigerende maatregelen opleggen:

- waarschuwing;
- berisping;
- verplichting om verzoeken tot uitoefening van rechten in te willigen;
- verplichting om verwerkingen in overeenstemming te brengen met de bepalingen van de GDPR;
- verplichting om een inbreuk in verband met de persoonsgegevens aan de betrokken persoon mee te delen;
- tijdelijke of definitieve verwerkingsbeperking, waaronder een verwerkingsverbod;
- verplichting tot rectificatie of wissing van persoonsgegevens;
- verplichting tot opschorting van gegevensstromen naar een derde land.

België heeft met de Gegevensbeschermingswet gebruik gemaakt van de door de GDPR geboden mogelijkheid om de overheid uit te sluiten van het regime van administratieve geldboeten, met uitzondering van de publiekrechtelijke rechtspersonen die goederen of diensten aanbieden op de markt.

7.2 Strafsancties

Op basis van de Gegevensbeschermingswet kunnen bepaalde inbreuken tevens strafrechtelijk beteugeld worden. Bovendien riskeert niet alleen de verwerkingsverantwoordelijke of verwerker een straf, maar tevens zijn aangestelde of gemachtigde. De verwerkingsverantwoordelijke of verwerker is weliswaar burgerrechtelijk aansprakelijk voor de betaling van boetes waartoe zijn aangestelde of gemachtigde is veroordeeld.

Voor de volgende inbreuken kan een geldboete van 2.000 EUR tot 120.000 EUR worden opgelegd:

- verwerking zonder wettelijke basis;
- overtreding van de basisbeginselen inzake verwerking van persoonsgegevens, met ernstige nalatigheid of kwaadwillig;
- handhaving van een verwerking waartegen een bezwaar is gemaakt, zonder dwingende wettige redenen;
- doorgifte van persoonsgegevens buiten de Europese Economische Ruimte zonder adequaatheidsbesluit of passende waarborgen, met ernstige nalatigheid of kwaadwillig;
- schending van een tijdelijke of definitieve verwerkingsbeperking opgelegd door de GBA;
- negeren van een corrigerende maatregel opgelegd door de GBA;
- belemmering van het toezicht of weerspannigheid ten aanzien van de GBA;
- gebruik van valse certificering of certificering waarvan de geldigheidsduur verstreken is.

Een onderneming die een persoon dwingt om toestemming te geven voor een verwerking van diens persoonsgegevens door gebruik te maken van feitelijkheden, geweld, bedreigingen, giften of beloften is strafbaar met een geldboete van 800 tot 160.000 EUR.

Verder kan ook de correctionele rechtbank bevelen dat een vonnis (of een uittreksel ervan) wordt gepubliceerd in een of meerdere dagbladen.

De opgeheven reglementering voorzag reeds in strafrechtelijke geldboetes, maar in de praktijk werden deze nauwelijks toegepast. Het niveau van deze geldboetes en het risico dat deze worden opgelegd is nu hoger.

Toch is het opmerkelijk dat het maximumbedrag van de strafrechtelijke geldboetes markant lager is dan dat van de administratieve geldboetes. In andere domeinen, zoals het sociaal strafrecht, is het immers gebruikelijk dat het niveau van administratieve boetes lager ligt dan de strafrechtelijke boetes, die als ultieme remedie gelden. De GBA had er in haar advies over het voorontwerp van Gegevensbeschermingswet aan herinnerd dat het vastgelegde sanctieniveau moet toelaten om doeltreffend, evenredig en afschrikkend te reageren. De praktijk zal moeten uitwijzen of deze sanctieniveaus effectief het gewenste effect zullen hebben. In elk geval zal het o.i. ook een impact hebben op de wisselwerking tussen enerzijds de GBA die de administratieve geldboetes kan opleggen en het openbaar ministerie die kan beslissen om te dagvaarden voor de correctionele rechtbank.

7.3 Samenloop tussen administratieve en strafrechtelijke procedures

Voor inbreuken waarvoor zowel een administratieve als een strafsanctie mogelijk is, heeft de Gegevensbeschermingswet een aantal procedureregels bepaald om te vermijden dat een onderneming beide sancties opgelegd krijgt voor diezelfde inbreuk.

Het openbaar ministerie is als eerste aan zet en kan een opsporingsonderzoek opstarten, een gerechtelijk onderzoek gelasten en/of strafvervolging voor de strafrechtbanken instellen. Het openbaar ministerie beschikt over een termijn van twee maanden vanaf de dag van ontvangst van het proces-verbaal om de opstart van een strafrechtelijke actie mee te delen aan de GBA. Tijdens deze termijn van twee maanden en wanneer het openbaar ministerie het dossier effectief opneemt, heeft de GBA niet (meer) de bevoegdheid om zijn corrigerende bevoegdheden uit te oefenen en zal een (hoge) administratieve geldboete bijgevolg niet kunnen worden opgelegd. Indien het openbaar ministerie deze termijn van twee maanden daarentegen laat verstrijken, zal enkel nog een administratieve sanctie mogelijk zijn.

De bovenstaande spelregels zullen echter enkel van toepassing zijn voor zover geen andere werkafspraken worden vastgelegd in een protocolakkoord tussen het openbaar ministerie en de GBA.

Brussel
Vorstlaan 280
1160 Brussel
Tel.: 02 761 46 00
Fax: 02 761 47 00

Luik
boulevard Frère Orban 25
4000 Luik
Tel.: 04 229 80 11
Fax: 04 229 80 22

Antwerpen
City Link
Posthofbrug 12
2600 Antwerpen
Tel.: 03 285 97 80
Fax: 03 285 97 90

Gent
Ferdinand Lousbergkaai 103
bus 4-5
9000 Gent
Tel.: 09 261 50 00
Fax: 09 261 55 00

Kortrijk
Ring Bedrijvenpark
Brugsesteenweg 255
8500 Kortrijk
Tel.: 056 26 08 60
Fax: 056 26 08 70

Hasselt
Kuringersteenweg 172
3500 Hasselt
Tel.: 011 24 79 10
Fax: 011 24 79 11

Partners with you.