[naam organisatie]

T.a.v. [naam of afdeling]

[straat en huisnummer of postbus]

[postcode + plaats]

[plaatsnaam], [datum] 2018

Dossiernummer/ons kenmerk: [invullen]

Uw kenmerk: [invullen of n.v.t.]

Telefoonnummer: [invullen]

E-mail: [invullen]

**Betreft: AVG en afspraken over uitwisseling persoonsgegevens en/of verwerking**

Geachte [naam],

Inleiding

[naam advocatenkantoor/bedrijfsnaam + eventueel entiteit], hierna te noemen: “[verwijzingsnaam invullen]”, verstrekt persoonsgegevens aan uw organisatie op basis van een wettelijke verplichting en/of taakuitvoering dan wel wisselt persoonsgegevens met uw organisatie uit. Vervolgens verwerkt uw organisatie zelfstandig deze persoonsgegevens. De eerder gemaakte afspraken met uw organisatie omtrent de (eenzijdige) verstrekking of uitwisseling van persoonsgegevens dienen in het kader van de nieuwe regelgeving op het gebied van privacy en gegevensbescherming te worden geactualiseerd.

Verandering in verplichtingen onder de AVG

De Algemene verordening gegevensbescherming (AVG) is een Europese wet die per 25 mei 2018 rechtstreeks van toepassing is en de Wet bescherming persoonsgegevens vervangt. Met de AVG is er nu één persoonsgegevensbeschermingswet voor de hele Europese Unie. De AVG regelt de rechtmatige en zorgvuldige omgang met persoonsgegevens. De AVG versterkt de positie van de betrokkenen. Hun privacyrechten worden uitgebreid en in bepaalde gevallen versterkt. Daarnaast krijgen organisaties die persoonsgegevens verwerken meer verplichtingen. Ook op [verwijzingsnaam invullen] rust de verplichting om aan te kunnen tonen aan de AVG te voldoen.

Nadere afspraken

In dit kader hecht [verwijzingsnaam invullen] als verwerkingsverantwoordelijke grote waarde aan het maken van afspraken met uw organisatie. Uw organisatie ontvangt van [verwijzingsnaam invullen] persoonsgegevens, die uw organisatie vervolgens zelfstandig verder verwerkt voor (een) eigen doeleinde(n). Voor deze verdere verwerking door uw organisatie bestaat geen verplichting om met u een verwerkersovereenkomst te sluiten. [verwijzingsnaam invullen] acht het in verband met zijn/haar eigen wettelijke verplichting en/of taakuitvoering en de verstrekking van persoonsgegevens aan uw organisatie dan wel uitwisseling van persoonsgegevens wel gewenst om in lijn met de AVG nadere afspraken met uw organisatie te maken over die verstrekking of uitwisseling. [NB: omschrijf in deze alinea uw specifieke situatie]

Wij/ik vragen u deze brief intern door te sturen naar de juiste persoon die privacy in zijn of haar portefeuille heeft, voor zover u zelf niet diegene bent. Daarnaast vragen wij/vraag ik uw aandacht om deze brief te (laten) ondertekenen, inclusief een paraaf op de bijlagen, door een daartoe bevoegde vertegenwoordiger van uw organisatie en deze zo snel mogelijk, maar uiterlijk binnen vier weken na dagtekening, aan ons/mij retour te zenden. Dit kan per email of per post [NB: kies zelf eigen communicatievorm].

Heeft u vragen, neem dan contact met ondergetekende op via de hierboven vermelde contactgegevens o.v.v. ‘reactie op brief aanvullende afspraken AVG’.

Met vriendelijke groet,

[naam advocatenkantoor/bedrijfsnaam],

[naam van de bevoegde persoon]

[titel/functie]

Bijlagen:

1. Afspraken

2. Overzicht verstrekte persoonsgegevens

3. Meldingsformulier Beveiligingsincident

4. Verklaring

**BIJLAGE 1.**

De volgende afspraken gelden tussen [naam advocatenkantoor/bedrijfsnaam] en [naam organisatie] (hierna: “ontvanger”) met betrekking tot de door [naam advocatenkantoor/bedrijfsnaam] verstrekte en nog te verstrekken persoonsgegevens (hierna: “persoonsgegevens”):

- [naam advocatenkantoor/bedrijfsnaam] verstrekt aan ontvanger uitsluitend persoonsgegevens op basis van een wettelijke grondslag of de bestaande samenwerkingsrelatie;

- ontvanger stelt voor de verdere verwerking van de persoonsgegevens zelf het doel en de middelen vast;

- ontvanger is zelf verwerkingsverantwoordelijke van de persoonsgegevens, die voor eigen doeleinden worden verwerkt;

- ontvanger draagt zorg voor strikte vertrouwelijkheid ter zake van bedoelde persoonsgegevens en treft daartoe (intern) afdoende maatregelen en voorzieningen;

- ontvanger waarborgt jegens [naam advocatenkantoor/bedrijfsnaam] deugdelijk gebruik van de persoonsgegevens en deze niet aan te wenden voor commerciële doeleinden;

- ontvanger waarborgt jegens [naam advocatenkantoor/bedrijfsnaam] dat persoonsgegevens niet aan een derde partij worden doorgestuurd buiten de kaders van de zelfstandig vastgestelde doelen van verwerking door ontvanger, behoudens voorafgaande expliciete schriftelijke toestemming van [naam advocatenkantoor/bedrijfsnaam], mede in verband met een eventueel afwijkend doel van verwerking door die derde partij;

- zowel [naam advocatenkantoor/bedrijfsnaam] als ontvanger ontwikkelen, implementeren en onderhouden een schriftelijk informatiebeveiligingsbeleid dat vereist dat beide partijen passende technische en organisatorische maatregelen nemen om persoonsgegevens, in het licht van de huidige stand van de techniek, te beschermen tegen inbreuken op beveiliging, vertrouwelijkheid of integriteit en andere ongeautoriseerde of onwettige vormen van (verdere) verwerking. Deze maatregelen zullen een passend veiligheidsniveau (moeten) garanderen om een op het risico – in dit geval enkel ten aanzien van de verstrekking van persoonsgegevens – afgestemd beveiligingsniveau te waarborgen;

- [naam advocatenkantoor/bedrijfsnaam] en ontvanger onderkennen dat de hiervoor bedoelde technische en organisatorische maatregelen in de loop van de tijd kunnen veranderen en dat effectieve beveiligingsmaatregelen regelmatige evaluatie en aanpassing van de maatregelen vereisen en dat zij derhalve regelmatig, dan wel periodiek, althans zo vaak als nodig, elkaar hierop aanspreken;

- zowel [naam advocatenkantoor/bedrijfsnaam] als ontvanger zorgen op basis van wederkerigheid voor adequate beveiligingsmaatregelen en treffen hiertoe de (wettelijk) noodzakelijke passende technische en organisatorische maatregelen ter zake van beveiligingsincidenten, waaronder datalekken. Waar mogelijk zullen zowel [naam advocatenkantoor/bedrijfsnaam] als ontvanger elkaar bijstand verlenen bij het vervullen van de verplichting om verzoeken te beantwoorden van betrokken natuurlijke personen die op grond van de AVG de hun toekomende privacyrechten uitoefenen;

- zodra de ene partij op de hoogte is van een beveiligingsincident – in dit geval enkel ten aanzien van de verstrekking van persoonsgegevens – moet die partij alle noodzakelijke en passende maatregelen nemen om de gevolgen van het beveiligingsincident te onderzoeken, te reduceren en te herstellen en de andere partij helpen ervoor te zorgen dat die andere partij kan voldoen aan de privacywetgeving en eventuele wettelijke en/of contractuele verplichtingen (zoals verplichtingen om derden in kennis te stellen, inclusief toezichthouders en betrokkenen) in verband met het beveiligingsincident. Dit betekent met zoveel woorden, dat partijen over en weer – in dit geval enkel ten aanzien van de verstrekking van persoonsgegevens, dus gericht op het transport van de data tot aan de poort van ontvanger – hun medewerking verlenen in het kader van het hiervoor gestelde en eventuele nadere instructies van de ene aan de partij adequaat zal opvolgen;

- zowel [naam advocatenkantoor/bedrijfsnaam] als ontvanger dienen zich te onthouden van het op enigerlei wijze verstrekken of delen van informatie over beveiligingsincidenten aan derde partijen en/of betrokkenen, behoudens voor zover de ene partij daartoe wettelijk verplicht is of partijen anderszins (tussentijds) schriftelijk zijn overeengekomen;

- de bij zowel [naam advocatenkantoor/bedrijfsnaam] als bij ontvanger aangewezen contactpersonen informeren de andere partij onverwijld over elke inbreuk in verband met persoonsgegevens, dus beveiligingsincident, zodra hiervan kennis is genomen. Een dergelijke kennisgeving mag mondeling plaatsvinden, maar moet altijd gevolgd worden door een schriftelijke bevestiging aan de andere partij met gebruikmaking van het als bijlage 3 bijgevoegde “Meldingsformulier Beveiligingsincident”;

- indien en voor zover de niet-nakoming van enige van de hierboven genoemde afspraken door een van de partijen leidt tot een onrechtmatige daad is artikel 6:162 BW van toepassing.

**BIJLAGE 2.**

Overzicht van door [naam advocatenkantoor/bedrijfsnaam] verstrekte persoonsgegevens aan ontvanger:

**BIJLAGE 3.**

Meldingsformulier Beveiligingsincident, waaronder een datalek

|  |  |
| --- | --- |
|  | Verwerkingsverantwoordelijke |
| Organisatie | [naam advocatenkantoor/bedrijfsnaam] |
| Naam | [naam invullen]  Bij afwezigheid: [naam invullen] |
| Functie |  |
| E-mail | [emailadres invullen] o.v.v. ‘Melding Beveiligingsincident’ |
| Telefoon | [invullen] |

|  |  |
| --- | --- |
|  | Verwerkingsverantwoordelijke - Ontvanger |
| Organisatie | [naam invullen] |
| Naam | [naam invullen]  Bij afwezigheid: [naam invullen] |
| Functie | [invullen] |
| E-mail | [invullen] |
| Telefoon | [invullen] |

**1. Melding**

**A**. Algemeen:

- Dag en tijdstip constatering of ontdekking van de inbreuk:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- Dag en tijdstip waarop melding plaatsvindt:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**B**. Contactgegevens melder:

- Naam:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- Functie:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- Emailadres:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- Telefoonnummer werk / mobiel:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**C**. Gegevens betrokken organisatie/bedrijf:

- Naam organisatie/bedrijf:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- Adres:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- Land:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- Welke partij is Verwerkingsverantwoordelijke en Verwerker:

o Verwerkingsverantwoordelijke

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

o Verwerker

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- Eventueel kenmerk of referentienummer van de hoofdovereenkomst en/of verwerkersovereenkomst:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

- Is aan deze organisatie / dit bedrijf verwerking van persoonsgegevens uitbesteed:

o Ja / nee (\* omcirkel wat van toepassing is)

o Korte toelichting:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**D**. Vindt de verwerking van persoonsgegevens binnen de EER plaats:

o Ja / nee (\* omcirkel wat van toepassing is)

o Korte toelichting:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**2.** Omschrijving van het incident waarbij de inbreuk op persoonsgegevens zich heeft voorgedaan:

**A.** Plaats waar de inbreuk zich (feitelijk) heeft voorgedaan:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**B.** Dag en tijdstip waarop de inbreuk waarschijnlijk plaatsvond:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**C.** Korte omschrijving van de inbreuk:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**D.** Aard van de inbreuk (denk aan verlies of diefstal van laptop, mobiele telefoon, tablet, usb-stick, mobiele harde schijf, een verkeerd verzonden email aan onbevoegd persoon, inbreuk op beveiliging zoals een hack van buitenaf, geen back-up gemaakt van data, of nog onbekend, etc.):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**E.** Omschrijf de groep betrokkenen (categorie) om wiens persoonsgegevens het gaat:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**F.** Hoeveel personen zijn betrokken bij de inbreuk, eventueel aangeven minimum/maximum:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

G. Geef aan om welk soort persoonsgegevens het gaat bij de inbreuk:

1.  Naam -, adres - en woonplaatsgegevens
2.  Telefoonnummers
3.  Emailadressen of andere adressen voor elektronische communicatie
4.  Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord,

klantnummer of het zogenaamde A-nummer)

1.  Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
2.  Burgerservicenummer (BSN) of sofinummer
3.  Paspoortkopieën of kopieën van andere legitimatiebewijzen
4.  Geslacht, geboortedatum en/of leeftijd
5.  Persoonsgegevens met gevoelige of bijzondere kenmerken, zoals ras of

etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid (medische gegevens), of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid

1.  Persoonsgegevens van minderjarigen
2.  Strafrechtelijke gegevens
3.  Tuchtrechtelijke gegevens
4.  Overige gegevens, namelijk (vul aan): [NB: denk aan hypotheekgegevens,

arbeidsgerelateerde gegevens, persoonsgegevens die in het kader van uw dienstverlening richting cliënten van belang zijn]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**H**. Welke (ernstige) gevolgen of risico’s kan de inbreuk hebben (of heeft deze) voor de persoonlijke levenssfeer van betrokkenen:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**3.** Omschrijving technische en/of organisatorische maatregelen ter bescherming:

**A.** Welke technische en/of organisatorische maatregelen zijn er getroffen om de inbreuk aan te pakken en herstellen, alsook eventuele verdere inbreuk(en) te voorkomen dan wel te beperken:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**B.** Welke personen of organisaties zijn – naast de onder punt 1 genoemde namen – (mogelijk) ook op de hoogte van de inbreuk:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**C.** Zijn de bij de inbreuk betreffende persoonsgegevens versleuteld, van encryptie voorzien, gehasht of op een andere manier ontoegankelijk en onbegrijpelijk voor daartoe onbevoegden gemaakt:

o Ja / nee (\* omcirkel wat van toepassing is)

o Korte toelichting op wijze van versleutelen:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**D.** Zijn er in aanvulling op 3.A t/m C redenen om aan te nemen dat de inbreuk zeer waarschijnlijk geen nadelige gevolgen of risico’s zal hebben (of heeft) voor de persoonlijke levenssfeer van betrokkenen:

o Ja / nee (\* omcirkel wat van toepassing is)

o Indien ja, dan graag korte toelichting:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**4.** Aanvullende informatie

**A**. Is er verdere (relevante) informatie die de Verwerkingsverantwoordelijke nodig kan hebben om te voldoen aan de wettelijke verplichtingen ten aanzien van de Meldplicht Datalekken, waaronder in ieder geval het (kunnen) doen van een eventuele melding bij de Autoriteit Persoonsgegevens en/of het informeren van betrokkene(n):

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Einde formulier

**BIJLAGE 4.**

Ik verklaar hiermee dat door ondertekening van deze brief de bovenstaande afspraken van toepassing zijn op de door [naam advocatenkantoor/bedrijfsnaam] op basis van een wettelijke verplichting en/of taakuitvoering verstrekte en nog te verstrekken persoonsgegevens aan onze/mijn organisatie dan wel uitwisseling van persoonsgegevens tussen onze organisaties. Daarbij treedt ontvanger als zelfstandig verwerkingsverantwoordelijke op. [NB: omschrijf hier uw specifieke situatie]

Organisatie:

………………………………………………………..

Naam:

………………………………………………………..

Functie:

………………………………………………………..

Datum:

………………………………………………………..

Handtekening:

………………………………………………………..