Bindende verwerkersverklaring VIVA Veterinary B.V

Deze verklaring is de bindende verwerkersverklaring van VIVA Veterinary B.V. Aan de hand van deze verklaring toont VIVA Veterinary B.V. in haar hoedanigheid als verwerker aan op welke wijze zij persoonsgegevens verwerkt en hoe zij de bescherming hiervan waarborgt.

VIVA Veterinary B.V., gevestigd te 3994 XZ te Houten aan de Pelmolen 20, hierna te noemen: "Verwerker" of "VIVA Vet", verklaart middels deze bindende verwerkersverklaring (hierna: "Verklaring") op welke wijze zij omgaat met de bescherming van persoonsgegevens in het kader van haar dienstverlening.

Verwerker verklaart als volgt:

Verwerking

1. Verwerker verklaart dat zij de persoonsgegevens in overeenstemming met de AVG op een behoorlijke en zorgvuldige wijze zal verwerken. Persoonsgegevens zullen enkel voor het doel waarvoor deze verstrekt zijn verwerkt worden en desgewenst op de schriftelijke instructie van verwerkingsverantwoordelijke, tenzij Verwerker op grond van geldende wet- en regelgeving verplicht is anders te handelen.

2. Verwerker verklaart dat indien op grond van een wettelijke verplichting, dan wel een rechterlijke uitspraak persoonsgegevens verstrekt dienen te worden, zij voorafgaand aan verstrekking de betreffende verwerkingsverantwoordelijke ter zake zal informeren.

3. Verwerker verklaart de persoonsgegevens enkel te bewaren zolang haar dienstverlening aan verwerkingsverantwoordelijke loopt en voor zover er geen andere wettelijke bewaartermijnen van toepassing zijn.

4. De verwerking van persoonsgegevens geldt uitsluitend voor de in bijlage I van deze Verklaring opgenomen categorieën van persoonsgegevens. Hierin is tevens opgenomen welke (groepen) medewerkers toegang tot de persoonsgegevens hebben, welke verwerkingen zijn toegestaan, alsmede de duur van de periode dat de persoonsgegevens opgeslagen worden.

5. Verwerker verklaart dat diens medewerkers enkel toegang tot de persoonsgegevens zullen hebben indien dat redelijkerwijs voor de uitoefening van hun werkzaamheden vereist is.

6. Indien Verwerker op enig moment tot de ontdekking komt dat de door verwerkingsverantwoordelijke in het praktijkmanagementsysteem van Verwerker ingevoerde (persoons-)gegevens niet enkel worden aangewend ten behoeve van de dagelijkse praktijkvoering van verwerkingsverantwoordelijke; de verwerking door verwerkingsverantwoordelijke verdergaat dan strikt noodzakelijk; de persoonsgegevens onrechtmatig zijn verkregen, dan wel inbreuk maken op rechten van derden zal Verwerker de nodige consequenties nemen teneinde de onrechtmatige verwerkingen stop te zetten dan wel te beperken.

7. Verwerker zal in het kader van de verwerkingsactiviteiten die zij voor verwerkingsverantwoordelijke verricht, voor zover redelijkerwijs mogelijk, medewerking verlenen aan de door verwerkingsverantwoordelijke op grond van de AVG na te komen verplichtingen ten aanzien van de rechten van een betrokkene.

8. Verwerker zal zorgdragen voor een goede beveiliging van de persoonsgegevens. Bij het nemen van beveiligingsmaatregelen neemt Verwerker passende maatregelen welke in overeenstemming zullen zijn met de stand van de techniek, de proportionaliteit tussen de beveiligingsmaatregelen en de aard van

de persoonsgegevens en de kosten die met de beveiligingsmaatregelen gemoeid zijn. Deze beveiligingsmaatregelen zijn in bijlage II van deze Verklaring opgenomen. Verwerker geeft echter geen garantie dat deze maatregelen onder alle omstandigheden doeltreffend zijn.

9. Verwerker zal een register, in de zin van artikel 30 lid 2 van de AVG, houden van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van verwerkingsverantwoordelijke verricht.

10. Verwerkingsverantwoordelijke kan de verwerking van persoonsgegevens door Verwerker te allen tijde (laten) controleren en zodoende nagaan of aan de in deze Verklaring opgenomen verplichtingen is voldaan. Verwerker zal hier, voor zover redelijkerwijs mogelijk, medewerking aan verlenen.

11. Verwerker zal uitsluitend op een rechtmatige grondslag gegevens verwerken die betrekking hebben op doorgiften van persoonsgegevens aan een land gevestigd buiten de Europese Unie of een internationale organisatie

Inbreuk in verband met persoonsgegevens

12. Verwerker verklaart verwerkingsverantwoordelijke tijdig in kennis te stellen van alle inbreuken in verband met persoonsgegevens, alsmede incidenten die op grond van wet- en regelgeving gemeld dienen te worden aan een toezichthouder of betrokkene. De verantwoordelijkheid voor de onverwijlde in kennisstelling van betrokkene en de betreffende toezichthouder binnen de daartoe ingevolge de AVG gestelde termijn ligt nimmer bij Verwerker.

13. Verwerker zal zorgdragen voor het ongedaan maken van de gevolgen van dergelijke inbreuken en incidenten, dan wel deze gevolgen te beperken voor zover redelijkerwijs mogelijk is.

14. Verwerker zal een logboek bijhouden van alle inbreuken in verband met persoonsgegevens, alsmede de genomen maatregelen ter stopzetting van de inbreuken of het beperken van uit de inbreuken voortvloeiende schade en kan verwerkingsverantwoordelijke hierin op het eerste verzoek inzage in verschaffen. Indien verwerkingsverantwoordelijke aanvullende informatie verzoekt, zal Verwerker, voor zover redelijk, hiertoe medewerking verlenen op een zo kort mogelijke termijn.

Geheimhouding

15. Verwerker verklaart dat zij, inclusief haar medewerkers en door haar ingeschakelde derden, verplicht zijn tot geheimhouding van de persoonsgegevens die zij verwerken, behoudens voor zover een bij, of krachtens de wet gegevens voorschrift tot verstrekking verplicht of de werkzaamheden van Verwerker daartoe noodzaken. Verwerker draagt er zorg voor dat een ieder, waaronder haar medewerkers en eventueel ingeschakelde derden, die in aanraking komt met persoonsgegevens contractueel gehouden is tot geheimhouding.

Subverwerkers

16. Indien Verwerker ter uitvoering van de overeenkomst die zij met verwerkingsverantwoordelijke heeft een subverwerker wenst in te schakelen, zal Verwerker er zorg voor dragen dat zij enkel een subverwerker inschakelt die afdoende waarborgen biedt ten aanzien van de bescherming van persoonsgegevens. Verwerker zal voor het inschakelen van een subverwerker voor zover redelijkerwijs benodigd schriftelijke toestemming vragen aan verwerkingsverantwoordelijke, welke toestemming niet op onredelijke gronden geweigerd mag worden. Indien Verwerker een subverwerker inschakelt, kan Verwerker verwerkingsverantwoordelijke inlichten over de beoogde veranderen inzake de toevoeging (dan wel vervanging) van een subverwerker, waarbij verwerkingsverantwoordelijke de mogelijkheid heeft hiertegen bezwaar te maken.

Aansprakelijkheid

17. In voorkomend geval zal de aansprakelijkheid van Verwerker conform het hiertoe bepaalde in artikel 82 van de AVG zijn.

18. Verwerker kan enkel aansprakelijk gesteld worden voor schade ontstaan na de inwerkintreding van deze Verklaring.

Overig

19. Deze Verklaring is slechts van toepassing in gevallen dat VIVA Vet in het kader van het ter beschikking stellen van haar praktijkmanagementsysteem als Verwerker in de zin van de Algemene Verordening Gegevensbescherming (AVG) aangemerkt kan worden. Indien op enig moment de dienstverlening aan een betreffende verwerkingsverantwoordelijke eindigt, kunnen er niet langer rechten aan deze Verklaring ontleend worden.

20. Daar waar in deze Verklaring terminologie uit de AVG is gebruikt, dient hieraan de betekenis te worden gegeven die de AVG hieraan geeft.

21. Deze Verklaring treedt in werking per 1 februari 2019.

22. Verwerker behoudt zich het recht voor deze Verklaring te allen tijde te wijzigen en/of aanvullen. Verwerker stelt verwerkingsverantwoordelijke op de hoogte van wijzigingen en/of aanvullingen.

23. Indien Verwerker met een verwerkingsverantwoordelijke een verwerkersovereenkomst overeengekomen is of ander wederkerig document dat de verplichtingen uit de AVG vastlegt, zal die verwerkersovereenkomst, dan wel wederkerig document prevaleren boven deze Verklaring.

Bijlage I – Categorieën persoonsgegevens

I. Categorieën persoonsgegevens

Verwerker verwerkt, in het kader van de overeenkomst met verwerkingsverantwoordelijke de volgende categorieën persoonsgegevens:

- NAW- en betaalgegevens van dierbezitters, voor zover ingevoerd door verwerkingsverantwoordelijke middels het praktijkmanagementsysteem van Verwerker;
- NAW- en betaalgegevens van veehouderijen, voor zover ingevoerd door verwerkingsverantwoordelijke middels het praktijkmanagementsysteem van Verwerker;
- NAW- en betaalgegevens van verwerkingsverantwoordelijke;
- NAW- en betaalgegevens van andere organisaties die dieren houden, voor zover ingevoerd door verwerkingsverantwoordelijke middels het praktijkmanagementsysteem van Verwerker.

Volledigheidshalve merkt Verwerker op dat voornoemde categorieën persoonsgegevens enkel door hem verwerkt worden voor zover verwerkingsverantwoordelijke deze persoonsgegevens noodzakelijk acht bij zijn praktijkmanagement en deze hiertoe heeft ingevoerd in het praktijkmanagementsysteem van Verwerker.

II. Groep(en) medewerkers

Verwerker verklaart dat enkel bevoegd personeel toegang heeft tot de verwerking van persoonsgegevens en dat alle bij Verwerker in dienst zijnde personen en/of door Verwerker ingeschakelde derden contractueel tot geheimhouding zijn verplicht. Medewerkers hebben geen toegang tot meer gegevens dan strikt noodzakelijk is voor de uitoefening van hun functie.

Verwerker stimuleert bewustzijn, opleiding en training ten aanzien van privacy- en informatiebeveiliging. Bovendien heeft Verwerker een gedragscode voor haar medewerkers waarin ten aanzien van de verwerking van persoonsgegevens regels zijn opgenomen waar iedere medewerker zich aan dient te houden.

Groep(en) medewerkers	Handelingen (verwerkingen) die zij uitvoeren met de persoonsgegevens	Doel van deze verwerkingen?
Medewerkers klantenservice	Enkel handelingen die zien op het adequaat beantwoorden van uw vraag.	Uw vragen zo goed mogelijk beantwoorden.
Medewerkers technische helpdesk	Slechts handelingen die benodigd zijn voor het verhelpen van (technische) problemen waar met het gebruik van het praktijkmanagementsysteem tegen aan wordt gelopen	Het verhelpen van (technische) problemen waar met het gebruik van het praktijkmanagementsysteem tegen aan wordt gelopen.
Medewerkers van IT	Slechts handelingen die gericht zijn op de beschikbaarheid, continuïteit en optimalisatie van het praktijkmanagementsysteem, zoals updates, conversies, installaties, back-ups en dergelijke.	Het gebruik van het praktijkmanagementsysteem en de daarmee samenhangende technische- en IT-gerelateerde aspecten up-to-date houden.
Medewerkers van de financiële afdeling / debiteurenbeheer	Het opstellen van facturen en opvolging van de betaling.	Het factureren van de vergoedingen/nota's en het bijhouden van de betalingen.

I. Bewaartermijnen

In afwijking van eventuele andere wettelijke bewaarplichten geldt dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld en verwerkt. In ieder geval geldt dat de fiscale bewaartermijn van de persoonsgegevens in het kader van de overeenkomst met verwerkingsverantwoordelijke 10 jaar is. Na ommekomst van deze periode worden de persoonsgegevens vernietigd.

Bijlage II – Beveiligingsmaatregelen

Verwerker is overeenkomstig de AVG verplicht aan te geven welke beveiligingsmaatregelen hij neemt ter bescherming van persoonsgegevens. Deze maatregelen zijn in overeenstemming met de stand van de techniek, de proportionaliteit tussen de beveiligingsmaatregelen, de aard van de persoonsgegevens en de kosten die met de beveiligingsmaatregelen gemoeid zijn. Indien Verwerker een subverwerker inschakelt, geeft verwerkingsverantwoordelijke hiertoe uitdrukkelijk zijn toestemming. Verwerker zal, in voorkomend geval, er voor zorgdragen dat enkel een subverwerker wordt ingeschakeld die afdoende waarborgen biedt ten aanzien van de bescherming van persoonsgegevens. Verwerker houdt een lijst van subverwerkers bij. Deze lijst ligt ter inzage op het kantoor van Verwerker.

I. Technische en organisatorische beveiligingsmaatregelen

Fysieke beveiliging en organisatorische maatregelen:

- ☐ er is een strikt sleutel- en codebeheer beleid;
- ☐ toegang tot niet-openbare gedeelten van gebouwen of beveiligingszones is alleen mogelijk na autorisatie daartoe;
- ☐ iedere uitgifte van toegangsmiddelen wordt geregistreerd;
- ☐ er is cameratoezicht;
- ☐ de fysieke toegang tot ruimten waar zich informatie- en ICT-voorzieningen bevinden is slechts voorbehouden aan bevoegde medewerkers;
- ☐ persoonsgegevens worden uitsluitend verwerkt in een gesloten, fysiek beveiligde omgeving met bescherming van bedreigingen van buitenaf, zoals onder andere een brandverzekering, alarminstallatie etc.;
- ☐ persoonsgegevens worden uitsluitend verwerkt op apparatuur waarbij maatregelen zijn genomen om de apparatuur fysiek te beveiligen en de continuïteit van de dienstverlening te verzekeren;
- ☐ bij beëindiging van het dienstverband van een medewerker worden alle bedrijfsmiddelen geretourneerd en worden autorisaties geblokkeerd;
- ☐ persoonsgegevens en programmatuur worden van apparatuur verwijderd of veilig overschreven, voordat de apparatuur wordt afgevoerd;
- ☐ externe hosting van data en/of services is onderworpen aan voorafgaande toestemming van het hoofd van de ICT-afdeling;
- ☐ er wordt een clean desk policy gehanteerd;
- ☐ beveiligingsmaatregelen hebben tevens betrekking op alle bedrijfsmiddelen;
- ☐ informatiedragers worden nooit onbeheerd achtergelaten;
- ☐ geen documenten op privé laptop opslaan;
- ☐ er is een noodstroomvoorziening.

Technische beveiligingsmaatregelen:

- ☐ de netwerkomgeving waarbinnen (persoons-)gegevens worden verwerkt is strikt beveiligd. Daarbij worden verkeersstromen gescheiden en zijn maatregelen geïmplementeerd tegen misbruik en aanvallen;
- ☐ alle gegevens zijn beveiligd door wachtwoorden, deze wachtwoorden zijn gebonden aan de laatste Microsoft systematiek;

- ☐ wachtwoorden worden periodiek vervangen;
- ☐ alle data die verstuurd wordt naar externe en/of publieke netwerken is voorzien van encryptie;
- ☐ de omgeving waarbinnen (persoons-)gegevens worden verwerkt wordt gemonitord;
- ☐ op wachtwoorden worden cryptografische maatregelen toegepast om deze gegevens veilig op te slaan;
- ☐ er wordt voor inlogprocessen gebruikgemaakt van versleutelde verbindingen;
- ☐ in het geval gebruik wordt gemaakt van het programma Team Viewer worden voor ieder gebruik nieuwe inlogcodes/wachtwoorden gebruikt;
- ☐ verbindingen worden beschermd tegen interceptie of beschadiging;
- ☐ gegevens op papier worden beschermd door een deugdelijke opslag en regeling voor de toegang tot archiefruimten;
- ☐ 'mobile code' wordt uitgevoerd in een logisch geïsoleerde omgeving om de kans op aantasting van de integriteit van het systeem te verkleinen. Deze wordt altijd uitgevoerd met minimale rechten zodat de integriteit van het host systeem niet aangetast wordt;
- ☐ up-to-date virusscanners;
- ☐ het netwerk wordt gemonitord en beheerd zodat aanvallen, storingen of fouten (tijdig) ontdekt en hersteld kunnen worden;
- ☐ de back-up en herstelprocedures worden regelmatig getest om de betrouwbaarheid ervan vast te stellen;
- ☐ versleutelde e-mail;
- ☐ geen onbeveiligde back-ups.