Algemene Verordening Gegevensbescherming (AVG)

De recreatiesector en de AVG:

nadere uitwerking verplichtingen voortvloeiende uit de AVG

RECRON , 6 januari 2018

Marcel Tap

Inhoud

pagina

De recreatiesector en de Algemene Verordening Gegevensbescherming (AVG)

Hoofdstuk 1 - Aanleiding

Op 25 mei 2018 treedt in de EU de Algemene Verordening gegevensbescherming (AVG) in werking. Daarmee wordt tegelijk de Nederlandse Wet Bescherming Persoonsgegevens buiten werking gesteld. De AVG werkt rechtstreeks door in de Nederlandse rechtspraktijk en daarmee ook in de recreatiesector; nadere regelgeving op nationaal niveau is dus niet nodig. De AVG brengt voor alle bedrijven die werken met persoonsgegevens (of bedrijfsgegevens die herleidbaar zijn naar persoonsgegevens) verplichtingen met zich mee. Zo ook voor recreatiebedrijven.

Dit document bevat de voor recreatiebedrijven relevante verplichtingen en geeft daarmee ook weer hoe recreatiebedrijven de bescherming van persoonsgegevens nader kunnen regelen en beleggen in de eigen organisatie, en wat er dient te gebeuren om te voldoen aan deze Europese wetgeving.

Geadviseerd wordt een volledig AVG-dossier aan te leggen (fysiek en/of digitaal), waarin alle zaken die van belang zijn in het kader van de gegevensverzameling en gegevensbescherming worden opgenomen en gedocumenteerd. Daarmee kan in voorkomende gevallen worden aangetoond dat wordt voldaan aan de verplichtingen die voort vloeien uit de AVG en kunnen hoge boetes van de Autoriteit Persoonsgegevens worden voorkomen.

Hoofdstuk 2 - De gegevens die vallen onder de AVG (Data-map)

De AVG verplicht om **in beeld te brengen** welke persoonsgegevens binnen het bedrijf worden verzameld en bewerkt. Dit betreft ook bedrijfsgegevens, die zijn te herleiden tot persoonsgegevens. Recreatiebedrijven kennen doorgaans verschillende soorten gegevens die (vaak) in geautomatiseerde bestanden en in fysieke bestanden zijn opgenomen. Hieronder volgt een (niet-limitatieve) opsomming van de mogelijke bedrijfs- en persoonsgegevens die doorgaans in recreatiebedrijven gebruikt en verwerkt worden:

1. **Gegevens van klanten/gasten**. Dit zijn NAW-gegevens van de klanten die een verblijf, activiteit of arrangement hebben geboekt , inclusief eventuele NAW-gegevens van familieleden of andere personen die aan die boeking gekoppeld zijn. Evenals andere relevante informatie die is verkregen van voornoemde klanten, zoals bijvoorbeeld emailadressen, bankrekening, geboortedata, enz. Deze gegevens worden doorgaans door het recreatiebedrijf opgenomen in het boekingssysteem c.q. een daaraan gekoppeld (ander) IT-systeem. Veelal is er ook een koppeling met financiële systemen.
2. **Gegevens van *potentiële* klanten**, dat wil zeggen personen of organisaties die hebben gevraagd om informatie over een verblijf, activiteit of arrangement, maar waarbij het niet tot een boeking is gekomen. Deze gegevens zijn doorgaans wel in IT-systemen opgenomen en worden in voorkomende gevallen mogelijk nog gebruikt voor marketingdoeleinden.

3. **Gegevens van leveranciers en adviseurs**, waarvan de recreatieondernemer gebruik maakt voor de bedrijfsvoering. Denk daarbij aan de horeca-leverancier, de energieleverancier, leverancier van linnenonderhoud of groenonderhoud, maar ook de accountant, de vaste bedrijfsadviseur en ook de bedrijfsgegevens van RECRON en de persoonsgegevens van de medewerkers van RECRON. Het gaat hierbij doorgaans om NAW-gegevens van bedrijven en contactpersonen, emailadressen, websiteadressen, KvK-gegevens, BTW-nummers, bankrekeningen, financiële gegevens, etc. Ook de gegevens van deze bedrijven c.q. personen zijn doorgaans opgenomen in een IT-systeem en vaak ook gekoppeld aan financiële systemen.

4. **Gegevens van stakeholders** waarmee het recreatiebedrijf c.q. de recreatieondernemer in verband met de bedrijfsvoering contacten onderhoudt of correspondentie voert. Het gaat om gegevens van bedrijven, instellingen en overheidsorganen c.q. contactpersonen van die stakeholders. Denk aan gegevens van collega-ondernemers, van gemeenteambtenaren, wethouders, burgemeester, ambtenaren van provincie, gegevens van omliggende en andere belanghebbende organisaties en andere organisaties en personen, zoals buren, verpachters, natuurorganisaties, milieuorganisaties, enz. In de meeste gevallen worden de bedrijfs- en persoonsgegevens verkregen via uitwisseling van visitekaartjes of via onderlinge (email) correspondentie of communicatie over het een of andere relevante onderwerp. De betreffende gegevens zijn soms opgenomen in een IT-systeem; in veel gevallen zitten de gegevens (ook) in een database die gekoppeld is aan een email-applicatie.

5. **Gegevens van personeelsleden**, werkzaam bij of voor het recreatiebedrijf. De dataset hierbij omvat veel: van NAW-gegevens tot bankrekening, geboortedatum, digitaal afschrift paspoort, partnergegevens (i.v.m. pensioenverzekering), enz. De gegevens zijn opgenomen in IT-systemen c.q. HR-systemen en vaak ook gekoppeld met financiële systemen of specifieke HR-systemen (zoals bv. urenregistratiesystemen). Tevens zijn er bij de recreatieondernemer fysieke dossiers aanwezig van de betreffende personeelsleden.

6. Er worden binnen recreatiebedrijven doorgaans geen bijzondere persoonsgegevens, zoals die van geaardheid of ras of strafrechtelijke gegevens, gebruikt, bewaard of bewerkt, maar mogelijk worden er wel **gegevens verzameld, bewaard en verwerkt van kinderen** (< 16 jaar). Dat hangt samen met de doelgroep van veel recreatiebedrijven (gezinnen met kinderen). Recreatiebedrijven richten zich in recreatieaanbod en hun animatieprogramma's vaak juist op die kinderen en verzamelen daartoe in voorkomende gevallen ook persoonsgegevens. Dit stelt bijzondere eisen aan het gebruik en de verwerking van persoonsgegevens. Zo moet toestemming van ouders of wettelijke vertegenwoordigers worden gevraagd voor het verzamelen en bewerken van gegevens van hun kinderen.

Hoofdstuk 3 - Grondslag en doeleinden van het verzamelen en bewerken van persoonsgegevens

Voor het mogen verzamelen en verwerken van persoonsgegevens **moet een grondslag** zijn. Die grondslag moet ook zijn **gedocumenteerd**.

Tenminste één van de volgende grondslagen moet aanwezig zijn:

a. **Toestemming**
Voor het verwerken van persoonsgegevens is (uitdrukkelijke) toestemming van de betrokken persoon nodig. Daarvoor gelden in het algemeen voorwaarden, zoals het vooraf en duidelijk (bv. aanvinken van een checkbox) toestemming verkrijgen voor de verzameling van de gegevens, het informeren van de betreffende persoon over het recreatiebedrijf en het doel van het gebruik van de gegevens (bij meerdere doelen elk doel aangeven), het informeren dat de toestemming altijd kan worden ingetrokken. Deze grondslag is in het bijzonder relevant in geval van verwerking van gegevens van personen met wie het niet tot een contractuele relatie is gekomen voor verblijf, activiteit of arrangement. Of in geval van verwerking van gegevens van personen met wie de contractuele relatie is geëindigd na afloop van het verblijf, de activiteit of het arrangement. Het advies is om uw boekingssystemen en marketingsystemen op dit punt te (laten) checken en zo nodig contact op te nemen met uw IT-leveranciers.

b. **Overeenkomst**
Het gaat hier om de gegevens die noodzakelijk zijn voor het voorbereiden of uitvoeren van de overeenkomst met de betrokken personen. Doorgaans dus om de gegevens van de klanten met wie een overeenkomst voor verblijf, activiteit of arrangement is gesloten; een leverancier of adviseur of een personeelslid. Als de overeenkomst is geëindigd mogen de gegevens alleen worden verwerkt als er toestemming is verleend door de betrokken persoon (zie a) of als er een andere grondslag is.

c. **Wettelijke verplichting**
In dit kader kunt u denken aan de verplichting om een nachtregister bij te houden of aan de verplichting dat u bij indiensttreding van een personeelslid een kopie van het identiteitsbewijs opneemt in het personeelsdossier of dat u relevante informatie over personeelsleden doorgeeft aan de belastingdienst.

d. **Vitaal belang**
Hier gaat het om gegevens die verband houden met een acute medische situatie. Daarvan zal in de meeste gevallen bij recreatiebedrijven geen sprake zijn.

e. **Gerechtvaardigd belang**
Deze grondslag zou van toepassing kunnen zijn, ingeval de gegevens nodig zijn voor het gerechtvaardigd belang van het recreatiebedrijf en het belang van de betrokken persoon niet voorgaat. Deze grondslag kan worden gehanteerd voor de verwerking van gegevens van personen die nog geen klant zijn, klant zijn geweest of stakeholders met wie geen contractuele relatie bestaat.

Er gelden wel vuistregels, zoals onder andere dat de gegevens echt nodig moeten zijn en dat ook dat als er gegevens kunnen worden gebruikt die niet herleidbaar zijn tot een persoon, deze gegevens moeten worden gebruikt. En voorts dat het belang van de persoon bij het verwerken van *bijzondere* persoonsgegevens (waaronder ook gegevens van kinderen) snel zwaarder weegt dan het bedrijfsbelang. Voorts geldt, dat als u de mogelijkheid biedt om bezwaar te maken tegen het gebruik van persoonsgegevens en de betrokken persoon maakt daarvan geen gebruik, dan weegt zijn privacybelang minder zwaar.

De ***grondslag*** voor het verzamelen en bewerken van klantgegevens is **dus doorgaans de contractuele relatie die leidt tot verblijf**, een activiteit en/of een arrangement.

Het ***doel*** van het verzamelen van deze gegevens is om met deze personen te kunnen communiceren over zaken die voor hen van belang zijn in het kader van hun verblijf c.a.

Ook een wettelijke verplichting vormt vaak de grondslag van het verzamelen en bewerken van persoonsgegevens (denk aan het zogenaamde nachtregister dat de recreatieondernemer moet verstrekken aan de gemeente).

De grondslag voor het verzamelen en bewerken van de *potentiële* klantgegevens, voor bijvoorbeeld marketingdoeleinden, kan dus zijn, dat de betreffende personen of organisaties op een moment expliciet belangstelling hebben getoond voor de diensten van een recreatieondernemer c.q. zich bij die ondernemer hebben gemeld met het verzoek hen op de hoogte te houden van het aanbod en de diensten van het recreatiebedrijf. Daarbij moet dan uitdrukkelijk toestemming zijn gegeven voor het gebruik en verwerken van de persoonsgegevens of er moet sprake zijn van een gerechtvaardigd belang (zie hiervoor onder sub d.). Het *doel* van het bewerken van deze gegevens is uiteraard om op enig moment tot een contractuele relatie te komen met die personen of organisaties.

De grondslag voor het bewerken van de gegevens van leveranciers en adviseurs, waaronder ook de (persoons)gegevens van de medewerkers van die leveranciers en adviseurs (zoals bijvoorbeeld RECRON), is dus doorgaans de bestaande en vaak voortdurende (contractuele) relatie met die leverancier of adviseur. En als die contractuele relatie er (even) niet meer is, dan is er vaak wel een gerechtvaardigd belang voor de verwerking van de persoonsgegevens. Het doel ervan is communicatie, opdrachtverstrekking, betaling van facturen, enz.

Voor de personeelsleden van het recreatiebedrijf is de arbeidsovereenkomst die met het bedrijf c.q. de recreatieondernemer is gesloten de grondslag voor de gegevensverzameling. Er is vanwege die relatie tevens een gerechtvaardigd belang en voor wat betreft een aantal gegevens van de betrokken personen ook een wettelijke verplichting. Het doel voor de gegevensverwerking behoeft geen nadere uitleg.

Het vastleggen van de grondslagen die van toepassing zijn en de doeleinden van de verwerking van gegevens in uw AVG-dossier is verplicht.

Hoofdstuk 4 - De verplichtingen

De AVG kent de nodige verplichtingen. In de eerste plaats betreft dat het in beeld brengen van de gegevens die worden verwerkt en de grondslagen en doeleinden (zie hiervoor). Voorts het in beeld brengen en nader uitwerken van een groot aantal andere zaken. De belangrijkste komen hieronder aan de orde met vermelding van de voor en bij recreatiebedrijven relevante aspecten.

1. **Identiteit van de (eind)verantwoordelijke functionaris(sen)**
   Leg vast wie eindverantwoordelijke is van het recreatiebedrijf. Doorgaans is (zijn) dat de eigena(a)r(en) of een parkmanager.

2. **De functionaris voor gegevensbescherming**
   De functionaris voor gegevensbescherming heeft als taak het toezicht houden op de toepassing en naleving van de AVG. De AVG verplicht in een aantal gevallen tot de aanstelling van een functionaris voor gegevensbescherming. Voor recreatiebedrijven geldt die verplichting in zijn algemeenheid **niet**. Er kan evenwel wel voor gekozen worden voor de bescherming van persoonsgegevens een functionaris aan te stellen, die dan bepaalde verantwoordelijkheden heeft, maar dit ontslaat de recreatieondernemer niet van zijn eindverantwoordelijkheid op dit vlak.

3. **Informatie over de ontvangers van de persoonsgegevens**
   Bepaal en documenteer wie binnen het recreatiebedrijf welke persoonsgegevens mogen verzamelen en bewerken. Zo zal een medewerker van de salarisadministratie wel de gegevens van personeelsleden moeten kunnen bewerken, maar is het de vraag of hij of zij klantgegevens mag of moet bewerken. En omgekeerd voor een medewerker die zich uitsluitend bezig houdt met het onderhoud op het recreatiebedrijf, zal waarschijnlijk moeten gelden, dat hij of zij uitsluitend gegevens mag verwerken van leveranciers die bij dat onderhoud betrokken zijn en geen gegevens mag inzien of bewerken van klanten of (andere) personeelsleden.

4. **Van wie worden gegevens ontvangen, verzameld of bewerkt?**
   De persoonsgegevens die hier bedoeld zijn, worden in het algemeen aangereikt door de desbetreffende personen zelf. Het kan daarbij ook gaan om gegevens van andere personen dan degene die de gegevens aanreikt. Denk aan gegevens van gezinsleden of (andere) medewerkers van een externe leverancier of adviseur. Voor bijzondere persoonsgegevens (zoals ras, geaardheid) en persoonsgegevens van kinderen gelden specifieke regels. Met name het laatste speelt bij veel recreatiebedrijven in verband met de aanwezigheid en registratie van kinderen op recreatiebedrijven en de deelname van kinderen aan animatieprogramma's op recreatiebedrijven.

5. **Aan wie worden gegevens doorgegeven?**
   Leg vast aan wie of welke organisaties of instanties u gegevens doorgeeft of verstrekt. Het kan zijn dat deze personen of organisaties de aan hen verstrekte gegevens ook weer zelf verwerken of doorgeven. Leg daarbij tevens per organisatie vast wat de grondslag is voor het doorgeven of verstrekken van de gegevens.

U kunt in dit verband denken aan de gegevens van uw klanten die opgenomen zijn in de IT-bestanden, die door een externe IT-leverancier of een datawarehouse worden bewaard. Maar denk ook aan de persoonsgegevens van uw klanten die u moet doorgeven aan overheidsinstanties i.v.m. belastingdoeleinden.

Ook als u ten behoeve van bijvoorbeeld een meting van klanttevredenheid persoonsgegevens doorgeeft aan een externe onderzoeker, dan moet u dat met benoeming van de grondslag en het doel vastleggen. Een ander voorbeeld is dat er persoonsgegevens van uw werknemers moeten worden doorgegeven aan de belastingdienst, de arbodienst of (in voorkomende gevallen) andere instanties. Ga uw werkprocessen na en leg een en ander vast in uw AVG-dossier.

6. **Doorgifte van gegevens buiten de EU? Opslag van gegevens buiten de EU?**
   Dit is in beginsel verboden volgens de AVG en bij recreatiebedrijven doorgaans niet aan de orde.

7. **Regels over teveel of te weinig gegevens en over de bewaartermijn van gegevens**
   U mag niet meer maar ook niet minder persoonsgegevens gebruiken dan noodzakelijk is voor het doel waarvoor u ze gebruikt. Als u bijvoorbeeld een geschil heeft met een klant of een leverancier dan moet u niet alleen uw eigen standpunten en argumenten vastleggen, maar ook de verkregen standpunten en argumenten van die klant of leverancier.
   Over bewaartermijnen zijn geen specifieke regels gesteld in de AVG, behalve dat daarvoor termijnen in de protocollen of uw AVG-dossier moeten worden opgenomen. Als regel geldt dat persoonsgegevens niet langer dan noodzakelijk voor het doel waarvoor ze worden verzameld worden bewaard. Soms zijn er van overheidswege bewaartermijnen van toepassing.

8. **Recht om inzage**
   Op verzoek hebben alle personen die in de IT-systemen van recreatiebedrijven staan recht op inzage van hun gegevens c.q. het recht op wijziging, rectificatie en wissen ervan. Dit recht dient in de privacyverklaring die doorgaans op de website van het recreatiebedrijf zal staan, te worden opgenomen.

9. **Data Protection Officer (DPO)**
   In sommige gevallen is de aanstelling van een DPO verplicht, in de regel bij meer dan 250 werknemers. Voor de meeste recreatiebedrijven geldt die verplichting dus niet.

10. **Bewerkersovereenkomsten**
    In verband met het verzamelen, bewaren, gebruiken en verwerken van (persoons)gegevens wordt vaak gebruik gemaakt van externe dienstverleners. Denk aan de leveranciers van uw boekingssoftware, uw ‘Cloud’-leveranciers, de leverancier(s) van uw financiële systemen en financiële dataopslag, uw arbodienst (die van u gegevens ontvangt), de dienstverlener die uw website host, het pensioenfonds, het SFR (KIKK), enz. Het is aan te bevelen de relaties en overeenkomsten met die partijen (die in de AVG bewerkers worden genoemd) zodanig in te richten dat deze AVG-proof zijn.

Over het algemeen zijn onderstaande onderwerpen in bewerkersovereenkomsten terug te vinden.

11. **Bewerking in overeenstemming met instructies verantwoordelijke**
    De bewerker mag de persoonsgegevens niet voor eigen doeleinden gebruiken, maar alleen om uitvoering te geven aan de instructies van de verantwoordelijke.

12. **Geheimhouding**
    In deze bepaling wordt aan de bewerker een geheimhoudingsplicht opgelegd, eventueel gecombineerd met een boetebeding. Overigens is opzettelijke niet-naleving van deze geheimhoudingsplicht strafbaar gesteld in het Wetboek van Strafrecht.

13. **Beveiligingsmaatregelen**
    De verantwoordelijke draagt zorg dat de bewerker passende technische en organisatorische maatregelen neemt om de persoonsgegevens te beveiligen tegen verlies e.d.

14. **Inschakelen van derden en onderaannemers**
    In de overeenkomst wordt vastgelegd of, en onder welke voorwaarden, de bewerker sub-bewerkers mag inschakelen.

15. **Locatie van de data**
    De verantwoordelijke moet weten in welke landen zijn data worden opgeslagen. Dit is mede van belang met het oog op de verplichtingen die gelden bij doorgifte van persoonsgegevens naar het buitenland.

16. **Audits**
    De verantwoordelijke moet kunnen controleren of de bewerker zich houdt aan de gemaakte afspraken. Dit gebeurt vaak in de vorm van een audit (onderzoek) door de verantwoordelijke of door een onafhankelijke derde. In de bewerkersovereenkomst kunnen partijen hier nadere afspraken over maken.

17. **Aansprakelijkheid**
    De wet bepaalt dat de verantwoordelijke kan worden aangesproken als iemand schade lijdt doordat wettelijke verplichtingen niet worden nageleefd. Dit geldt zelfs als de schade het gevolg is van nalatigheid van de bewerker, die in dat geval ook zelfstandig aansprakelijk is. Het is verstandig in de bewerkersovereenkomst heldere afspraken te maken over deze verdeling.

    Het advies voor dit moment aan u is om **uw dienstverleners voor een bewerkersovereenkomst te laten zorgen** en hen te vragen daarvoor een concept overeenkomst op te stellen. In de bijlagen is een voorbeeld van een IT-leverancier uit de sector opgenomen.

18. **Geheimhouding**
    Uw Medewerkers zijn in beginsel verplicht tot geheimhouding van (alle) zaken waarmee zij in hun werk te maken krijgen. In de cao (Dag-)Recreatie is daartoe een algemene bepaling opgenomen. Die bepaling is echter niet getoetst aan de AVG. Het is aan te bevelen aanvullend daarop nog een extra AVG-clausule op te nemen in de arbeidsovereenkomsten van de medewerkers die persoonsgegevens verzamelen en verwerken.

19. **Privacy Impact Assessment (PIA)**
    Het doel van een PIA is om de risico's in beeld te brengen die verband houden met het verzamelen en bewerken van persoonsgegevens en er voor te zorgen dat die risico's worden gemitigeerd. In sommige gevallen is het verplicht PIA's uit te voeren, namelijk als de gegevensverwerking een hoog risico met zich mee brengt. In de regel zal deze verplichting voor recreatiebedrijven niet van toepassing zijn.

20. **Beveiliging systemen met persoonsgegevens**
    Het is van belang de nodige aandacht te besteden aan de beveiliging van de IT-systemen waarin persoonsgegevens zijn opgenomen. De toegang tot deze systemen moet beperkt worden tot medewerkers, die deze gegevens nodig hebben voor hun werkzaamheden en daarvoor dan uitdrukkelijk geautoriseerd moeten zijn. Toegang op systemen wordt bij voorkeur via een beveiligingsscript ingeregeld (gebruikersnaam/password). Medewerkers die uit dienst gaan, moeten direct worden afgevoerd uit de systemen.

    De computers, laptops en databases die worden gebruikt voor de opslag en verwerking van persoonsgegevens moeten zijn beveiligd tegen aanvallen van buitenaf , via virus- en malwareprogramma's.

    De beveiliging van de bestanden met bedrijfs- en persoonsgegevens die (extern) in de 'cloud' staan, moet eveneens afdoende zijn geregeld door de desbetreffende externe dienstverleners. Het is aan te bevelen dit nader te regelen via de bewerkersovereenkomst als bedoeld onder nr. 10.

21. **Datalekken**
    Datalekken moeten worden gemeld aan de **Autoriteit Persoonsgegeven in Den Haag**. Hiervoor dient een protocol en/of een draaiboek Datalekken te worden gemaakt. In de bijlagen is een voorbeeld opgenomen.

22. **Privacy verklaring**
    De AVG verplicht tot een privacyverklaring. Het is aan te bevelen een privacy verklaring te maken en die toe te voegen aan uw website. In de bijlagen is daarvan een voorbeeld opgenomen.

23. **Privacy compliance maken van processen**
    Het is aan te bevelen alle bedrijfsprocessen die plaatsvinden te doorlopen en privacy-compliance te maken.

Dat kan door het verzamelen, bewaren en bewerken van gegevens op te knippen in diverse de diverse processen die binnen het recreatiebedrijf kunnen worden onderscheiden: zoals bijvoorbeeld de aanvraag voor het verzenden van informatie over een verblijf op het recreatiebedrijf; een boeking; een aankomst en de daarbij behorende gegevensverzameling; een betaling, enz.

24. **Inrichten Loketfunctie**
    Voor zowel de eigen medewerkers als externen, waaronder klanten, leveranciers en andere stakeholders, zal een informatiepunt moeten worden ingericht waar privacy-vragen kunnen worden neergelegd. Het heeft de voorkeur dat dit op voldoende hoog niveau in de organisatie (bijvoorbeeld bij een leidinggevende) wordt belegd en ingeregeld.

25. **Training medewerkers**
    Het is aan te bevelen om voor de medewerkers van het recreatiebedrijf een werksessie te organiseren om de betekenis en uitwerking van de AVG in de organisatie uit te leggen.

Hoofdstuk 5 - Checklist en actielijst

Uit de voorgaande lijst van verplichtingen volgt dat u mogelijk de nodige acties moet initiëren. Hieronder zijn die alle eventuele acties nog eens in tabelvorm samengevat.

Verplichting	**Noodzakelijke actie**	**Uitvoering door**	**Gewenste datum gereed**	**Datum gereed**
Functionaris gegevensbescherming	Aanwijzen indien noodzakelijk	meestal niet noodzakelijk		
Beleid ten aanzien van gegevensverstrekking aan derden	bepalen	Directie/leiding recreatiebedrijf		
Privacyverklaring	Maken/aanpassen en op website plaatsen	Voorbeeld in bijlage		
Bewerkers-overeenkomsten	In beeld brengen externe partijen en regelen dat deze partijen bewerkersovereenkomsten aanbieden	Bij voorkeur door: Externe dienstverleners		
Geheimhouding medewerkers	Aanvullende bepaling arbeidsovereenkomst	Voorbeeld in bijlage		
Beveiliging IT-systemen en bestanden	Check beveiliging (ook bij externen); regelen in bewerkersovereenkomsten	IT-functionaris		
Compliance	Processen doorlopen en AVG proof maken	Directie/leiding recreatiebedrijf		
Loketfunctie	Inrichten loket (aanwijzen verantwoordelijke) en communicatie dienaangaande	Directie/leiding recreatiebedrijf		
Datalekken	maken protocol en draaiboek datalekken	Voorbeeld in bijlage		
Training medewerkers	Organiseren werksessie	Directie/leiding recreatiebedrijf		

Bijlagen:
1. Voorbeeld Privacyverklaring
2. voorbeeld Geheimhoudingsverklaring
3. Voorbeeld Protocol datalekken

4. Voorbeeld Verwerkersovereenkomst

Bijlage 1 - Voorbeeld Privacyverklaring

Wij respecteren de privacy van bezoekers van de website en dragen er zorg voor dat de persoonlijke informatie die u ons verschaft vertrouwelijk wordt behandeld. Verwerking van de persoonsgegevens gebeurt op een wijze, die in overeenstemming is met de eisen die de Wet Bescherming Persoonsgegevens stelt.

Doeleinden van de gegevensverwerking
Uw persoonsgegevens worden door ons verwerkt voor het aangaan en uitvoeren van overeenkomsten ter zake juridische diensten en het beheren van de daaruit voortvloeiende relaties, met inbegrip het uitvoeren van activiteiten gericht op de vergroting van het klantenbestand.
Als u een contact- of aanmeldformulier op de website invult, of ons een e-mail stuurt, dan worden de gegevens die u ons toestuurt bewaard zolang als naar de aard van het formulier of de inhoud van uw e-mail nodig is voor de volledige beantwoording en afhandeling daarvan.

Klikgedrag en bezoekgegevens
Op de website worden algemene bezoekgegevens bijgehouden. In dit kader kan met name het IP-adres van uw computer, de eventuele gebruikersnaam, het tijdstip van opvraging en gegevens die de browser van een bezoeker meestuurt, worden geregistreerd en worden gebruikt voor statistische analyses van bezoek- en klikgedrag op de website. Tevens optimaliseren wij hiermee de werking van de website.
Wij proberen deze gegevens zo veel mogelijk te anonimiseren. Deze gegevens worden niet aan derden verstrekt.

Google Analytics
Wij maken gebruik van Google Analytics om bij te houden hoe gebruikers de website gebruiken. De aldus verkregen informatie wordt, met inbegrip van het adres van uw computer (IP-adres), overgebracht naar en door Google opgeslagen op servers in de Verenigde Staten.
Google gebruikt deze informatie om bij te houden hoe onze website gebruikt wordt, om rapporten over de website aan ons te kunnen verstrekken en om haar adverteerders informatie over de effectiviteit van hun campagnes te kunnen bieden. Google kan deze informatie aan derden verschaffen indien Google hiertoe wettelijk wordt verplicht, of voor zover deze derden de informatie namens Google verwerken. Wij hebben hier geen invloed op.

Facebook en Twitter (social media)
Op de website zijn knoppen opgenomen om pagina's te kunnen promoten of delen op sociale netwerken zoals Facebook en Twitter. Deze knoppen worden gerealiseerd door code die wordt aangeleverd door Facebook en Twitter zelf. Deze code plaatst onder meer een cookie.
Leest u de privacyverklaring van Facebook en van Twitter (welke regelmatig kunnen wijzigen) om te zien wat zij met uw persoonsgegevens doen die zij met deze code verwerken.
Dit geldt ook voor andere social media kanalen.

Nieuwsbrief
Wij bieden een nieuwsbrief waarmee wij geïnteresseerden willen informeren over nieuws op het gebied van ICT- en internetrecht, onze diensten en aanverwante zaken. Uw e-mailadres wordt alleen met uw expliciete toestemming toegevoegd aan de lijst van abonnees. Iedere nieuwsbrief

bevat een link waarmee u zich kunt afmelden. Het abonneebestand van de nieuwsbrief wordt niet aan derden verstrekt.

Gebruik van cookies
Wij maken bij het aanbieden van elektronische diensten gebruik van cookies. Een cookie is een eenvoudig klein bestandje dat met pagina's van deze website wordt meegestuurd en door uw browser op de harde schijf van uw computer wordt opgeslagen. Daarmee kunnen wij onder andere verschillende opvragingen van pagina's van de website combineren en het gedrag van gebruikers analyseren. U kunt het gebruik van deze cookies weigeren, hoewel dit de functionaliteit en het gebruiksgemak van de website kan beperken.

Inzage, correctie en recht van verzet
Indien u een relatie met ons bedrijf heeft, heeft u na schriftelijk verzoek de mogelijkheid uw persoonlijke gegevens in te zien. Indien het door ons verstrekte overzicht onjuistheden bevat, kunt u ons schriftelijk verzoeken de gegevens te wijzigen of te laten verwijderen. Daarnaast kunt u ons schriftelijk op de hoogte stellen, indien u niet wilt worden benaderd met informatie over onze producten en diensten door dit te melden bij navolgend adres:
[Naam en adresgegeven bedrijf]

Aanpassen privacy statement
Wij behouden ons het recht voor deze privacy statement aan te passen. Wijzigingen zullen op deze website worden gepubliceerd.

Bijlage 2 - Voorbeeld geheimhoudingsverklaring (opnemen in arbeidsovereenkomst of op te maken als aparte overeenkomst)

Geheimhoudingsplicht: gegevens, waaronder persoonsgegevens en eigendommen van werkgever.

Op de geheimhoudingsverplichting voor werknemer en werkgever is de Algemene Verordening Gegevensbescherming (AVG) van toepassing.

De werknemer verplicht zich zowel tijdens de duur van de arbeidsovereenkomst als na beëindiging daarvan zich te onthouden van het doen van enige mededeling aan derden, in welke vorm dan ook, hetzij direct, hetzij indirect, aangaande enige bijzonderheid het bedrijf van werkgever of aan haar gelieerde maatschappijen betreffende, of daarmee verband houdende, waarvan de werknemer redelijkerwijs kan begrijpen dat zulks niet bestemd is voor kennisname door derden.

De werknemer is gehouden data, gegevens, informatie en alles wat hem of haar in het kader van de uitvoering van de arbeidsovereenkomst ter kennis komt, vertrouwelijk te behandelen. Op het gebruik van vorenbedoelde data, gegevens en informatie c.a. is de AVG van toepassing.

Alle zaken, waaronder begrepen schriftelijke stukken en fotokopieën daarvan, alsmede geautomatiseerde gegevensdragers (waaronder computerdiskettes) die de werknemer van of ten behoeve van werkgever tijdens de arbeidsovereenkomst onder zich krijgt, zijn en blijven eigendom van werkgever. De medewerker zal deze zaken op het eerste verzoek van werkgever, doch in elk geval op het tijdstip waarop de arbeidsovereenkomst eindigt, wederom aan werkgever ter beschikking stellen.

Het niet nakomen of veronachtzamen van de verplichtingen als hiervoor bedoeld kan leiden tot arbeidsrechtelijke consequenties.

Bijlage 3 - Protocol meldplicht datalekken

De Wet Bescherming Persoonsgegevens (die per 25 mei 2018 wordt vervangen door de Algemene Verordening Gegevensbescherming (AVG) bevat de plicht om een datalek te melden bij de Autoriteit Persoonsgegevens (https://autoriteitpersoonsgegevens.nl/).

Bij een datalek is sprake van een inbreuk op de beveiliging van persoonsgegevens. Voorbeelden: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop, een inbraak in een databestand door een hacker of het ten onrechte verstrekken van persoonsgegevens aan derden.

Mocht u een datalek constateren in uw organisatie of vermoeden dat hiervan sprake is, dan kunt u aan de hand van de volgende vragen bepalen of u dit moet melden bij de Autoriteit Persoonsgegevens en de betrokkenen (degenen van wie de persoonsgegevens zijn gelekt).

1. Is de meldplicht datalekken van toepassing?
2. Is een gebeurtenis te beschouwen als een datalek?
3. Moet het datalek worden gemeld aan de Autoriteit Persoonsgegevens?
4. Hoe en wanneer moet het datalek worden gemeld aan de Autoriteit ?
5. Moet het datalek ook worden gemeld aan de betrokkene
6. Hoe en wanneer moet het datalek worden gemeld aan de betrokkene?
7. Welke gegevens moeten worden vastgelegd?

Ad 1. Is de meldplicht datalekken van toepassing?
Dat is het geval indien:

a. sprake is van verwerking van persoonsgegevens (elk gegeven betreffende een geïdentificeerde of identificeerbare persoon, zoals NAW-gegevens, IP-adressen en foto's). Verwerking van persoonsgegevens betreft elke handeling met betrekking tot persoons-gegevens, zoals het verzamelen, vastleggen, ordenen, raadplegen en verspreiden.

b. u de eindverantwoordelijke bent. Als u bij de verwerking derden inschakelt, blijft u met betrekking tot de meldplicht de eindverantwoordelijke.

Ad 2. Wanneer is een gebeurtenis te beschouwen als een datalek?
Dat is het geval indien:

a. sprake is van een inbreuk op de beveiliging, dat wil zeggen dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan, en

b. bij de inbreuk persoonsgegevens verloren zijn gegaan of redelijkerwijs niet kan worden uitgesloten dat er persoonsgegevens onrechtmatig zijn verwerkt, waaronder moet worden begrepen de aantasting van de persoonsgegevens, onbevoegde kennisneming, wijziging of verstrekking daarvan.

Ad 3. Moet het datalek worden gemeld aan de Autoriteit Persoonsgegevens?
Een datalek moet worden gemeld aan de Autoriteit Persoonsgegevens indien sprake is van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Dat is het geval indien één van de volgende situaties aan de orde is:

a. Persoonsgegevens van gevoelige aard zijn gelekt, zoals gegevens betreffende iemands levensovertuiging of godsdienst, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging of strafrechtelijke persoonsgegevens. Het kan ook gaan om persoonsgegevens die anderszins van gevoelige aard zijn, zoals gegevens over de financiële of economische situatie van de betrokkene; gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene; gebruikersnamen, wachtwoorden en andere inloggegevens; gegevens die kunnen worden misbruikt voor (identiteits-) fraude; gegevens uit DNA-databanken; gegevens waar een bijzondere, wettelijk bepaalde geheimhoudingsplicht op rust; en gegevens die onder een beroepsgeheim vallen.

b. De aard en omvang van de inbreuk leiden tot (een aanzienlijke kans op) ernstige nadelige gevolgen. Relevante vragen hierbij zijn: Gaat het om veel persoonsgegevens per persoon of om gegevens van grote groepen? Zijn de beslissingen die o.b.v. de verwerkte persoonsgegevens worden genomen ingrijpend? Worden de persoonsgegevens binnen ketens (zoals binnen de overheid) gedeeld? Gaat het om persoonsgegevens van kwetsbare groepen?

Ad 4. Hoe en wanneer moet het datalek worden gemeld aan de Autoriteit Persoonsgegevens?
De Autoriteit Persoonsgegevens heeft voor de melding een webformulier beschikbaar. Het datalek moet onverwijld worden gemeld. Dit houdt in dat de verantwoordelijke, na het ontdekken van een mogelijk datalek, enige tijd mag nemen voor nader onderzoek teneinde een onnodige melding te voorkomen. De termijn voor het melden begint te lopen op het moment dat de verantwoordelijke of een bewerker op de hoogte raakt van een incident dat mogelijk onder de meldplicht datalekken valt. Zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking, moet een melding worden gedaan, tenzij op dat moment inmiddels uit onderzoek is gebleken dat het incident niet onder de meldplicht datalekken valt.

Ad 5. Moet het datalek ook worden gemeld aan de betrokkene (degene van wie de persoonsgegevens zijn gelekt)?
Het datalek hoeft niet te worden gemeld aan de betrokkene indien één van de volgende situaties zich voordoet:

a. er zijn passende technische beschermingsmaatregelen genomen waardoor de persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens, bijvoorbeeld door adequate encryptie (versleuteling) en hashing (het omzetten van gegevens in een unieke code);

b. andere technische beschermingsmaatregelen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten, bijvoorbeeld door een tijdige en adequate remote wiping (het op afstand wissen van de gegevens die op een apparaat staan) en pseudonimisering (technische maatregelen om te voorkomen dat de persoonsgegevens worden gekoppeld aan de oorspronkelijke identiteit van de betrokkene);

c. het is onwaarschijnlijk dat het datalek ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene: als persoonsgegevens van gevoelige aard zijn gelekt, moet sowieso worden gemeld;

d. er zijn andere zwaarwegende redenen om de melding aan de betrokkene achterwege te laten.

Ad 6. Hoe en wanneer moet het datalek worden gemeld aan de betrokkene?
In de kennisgeving aan de betrokkene moet in ieder geval worden vermeld: de aard van de inbreuk; de instanties waar de betrokkene meer informatie over de inbreuk kan krijgen (contactgegevens) en de maatregelen die zijn aanbevolen om de negatieve gevolgen van de inbreuk te beperken. Het datalek moet onverwijld worden gemeld aan de betrokkene. Dit houdt in dat de verantwoordelijke, na het ontdekken van een mogelijk datalek, enige tijd mag nemen voor nader onderzoek zodat betrokkene op een behoorlijke en zorgvuldige manier kan worden geïnformeerd.

Ad 7. Welke gegevens moeten worden vastgelegd?
Er moet een overzicht worden bijgehouden van alle datalekken die onder de meldplicht vallen, dus datalekken die aan de Autoriteit Persoonsgegevens moeten worden gemeld. Per datalek bevat het overzicht in ieder geval de gegevens omtrent de aard van de inbreuk en, indien aan de betrokkene is gemeld, de tekst van de kennisgeving. De bewaartermijn van dit overzicht bedraagt minimaal een jaar.

Sancties
Bij overtreding van de meldplicht datalekken kan de Autoriteit Persoonsgegevens een bestuurlijke boete van ten hoogste € 820.000,- opleggen. Indien de overtreding niet opzettelijk is gepleegd en geen sprake is van ernstig verwijtbare nalatigheid, dan zal de Autoriteit Persoonsgegevens eerst een bindende aanwijzing opleggen.

Aanbevelingen

- Als u de verwerking geheel of gedeeltelijk laat uitvoeren door een bewerker, moet u als verantwoordelijke maatregelen nemen om ervoor te zorgen dat u in staat blijft de meldplicht datalekken na te komen. Daartoe kunnen met de bewerker afspraken worden gemaakt. Deze afspraken moeten schriftelijk worden vastgelegd, of in een andere, gelijkwaardige vorm. Denk hierbij aan de volgende onderwerpen: Gaat de bewerker u informeren over alle incidenten? Hoe en wanneer vindt deze informatieverstrekking plaats? Gaat de bewerker eventueel zelf meldingen doen aan de Autoriteit Persoonsgegevens? Wordt u geïnformeerd over door de bewerker getroffen verbetermaatregelen?
- Het is aan te bevelen om intern een procedure te ontwikkelen die medewerkers een praktisch handvat biedt hoe te handelen bij een (vermoeden van een) datalek. In deze interne procedure kunnen de volgende onderwerpen aan bod komen: Aan wie en binnen welke termijn moet een (mogelijk) datalek worden gemeld? Door wie en hoe wordt onderzoek gedaan naar de aard en de ernst van het incident? Wie verzorgt de eventuele melding aan de Autoriteit Persoonsgegevens en de betrokkenen? Wie is intern waarvoor verantwoordelijk?
- In het geval van een datalek kan er een vermoeden zijn van strafbaar handelen. Zo is bijvoorbeeld hacken strafbaar gesteld. Wanneer er aanwijzingen voor hacken zijn, dan is er alle aanleiding om daarvan aangifte te doen bij de politie.

Bron: Van Iersel Luchtman Advocaten, Breda en Den Bosch (www.vil.nl)

Bijlage 4 - Voorbeeld Verwerkersovereenkomst (bron: STERC B.V.)

Contractspartijen

NAAM (RECREATIE)BEDRIJF, gevestigd aan STRAAT, POSTCODE+PLAATS, geregistreerd bij de Kamer van Koophandel onder nummer XXXXXXXX, Bevoegd vertegenwoordigd door NAAM, treedt in deze overeenkomst op als verantwoordelijke, hierna te noemen de opdrachtgever

en

NAAM (IT) BEDRIJF gevestigd aan STRAAT, POSTCODE + PLAATS, , geregistreerd bij de Kamer van Koophandel onder nummer XXXXXXX, vertegenwoordigd door NAAM, treedt in deze overeenkomst op als verwerker, hierna te noemen de opdrachtnemer.

Definities

- *Persoonsgegevens:* Alle informatie welke het mogelijk maakt een natuurlijke persoon direct of indirect te kunnen identificeren.
- *Verantwoordelijke:* De partij die doel en middelen voor de verwerking bepaalt.
- *Verwerker:* De partij die in opdracht van de verantwoordelijke ten behoeve van de verantwoordelijke persoonsgegevens verwerkt.
- *Subverwerker*: De partij die door de verwerker ingeschakeld wordt om ten behoeve van de verantwoordelijke persoonsgegevens te verwerken.
- *Betrokkene:* De partij welke op grond van de persoonsgegevens identificeerbaar is.
- *Derde:* De partijen welke niet zijn de verantwoordelijke, betrokkenen of (sub)verwerker, noch de personen welke onder rechtstreeks gezag van de verantwoordelijke of verwerker gemachtigd zijn de gegevens te verwerken.

Uitgangspunten

Uit de Verordening (EU) 2016/679, hierna te noemen, Algemene Verordening Gegevensbescherming, volgt de verplichting tot het opstellen van deze aanvullende overeenkomst, de verwerkersovereenkomst, waarin de plichten van partijen zijn vastgelegd met betrekking tot het verwerken van persoonsgegevens welke voortvloeien uit de overeengekomen dienstenovereenkomst.

De opdrachtnemer levert een dienst in opdracht van de opdrachtgever. Deze dienst is gespecificeerd in een separate dienstenovereenkomst tussen de opdrachtnemer en de opdrachtgever waar de algemene voorwaarden, zoals overeengekomen tussen partijen, eveneens deel van uitmaken.

Samenvattend bestaat deze dienst uit het (door)ontwikkelen en hosten van een web applicatie voor de opdrachtgever.

De opdrachtnemer zal bij de uitvoering van haar dienst persoonsgegevens verwerken in de hoedanigheid van verwerker als bedoeld in de Algemene Verordening Gegevensbescherming. Deze overeenkomst heeft tot doel om nadere afspraken vast te leggen over de uitvoering van de verwerking van persoonsgegevens door de opdrachtnemer, met name het onderwerp en de duur van de verwerking, het doel van de verwerking, het soort persoonsgegevens, en de rechten en verplichtingen van de opdrachtgever.

Artikel 1 - Doel en middelen van verwerking

1. De opdrachtnemer verwerkt uitsluitend gegevens in opdracht van de opdrachtgever ten behoeve van de doelen die bepaald zijn door de opdrachtgever. De opdrachtnemer heeft daarbij geen zelfstandige zeggenschap over hoe de persoonsgegevens gebruikt worden.
2. De opdrachtgever bepaalt uitsluitend de middelen waarmee de persoonsgegevens verwerkt worden. De opdrachtnemer faciliteert slechts technisch de middelen waarmee de verwerking plaatsvindt.
3. In bijlage “Doelen en middelen” zijn de doelen en middelen van de verwerkingen van persoonsgegevens nader gespecificeerd.
4. De persoonsgegevens welke worden verwerkt worden direct door de opdrachtgever verstrekt of indirect in opdracht en onder verantwoordelijkheid van de opdrachtgever verkregen.
5. De opdrachtgever staat ervoor in dat de verwerking van persoonsgegevens die in opdracht van en ten behoeve van haar vastgestelde doelen, rechtmatig geschiedt.
6. De opdrachtnemer verwerkt de verkregen persoonsgegevens nimmer ten behoeve van eigen doelen waardoor zij nimmer als verantwoordelijke kan worden beschouwd.

Artikel 2 – Duur opslag van persoonsgegevens

De opdrachtgever bepaalt dat de duur van de opslag van persoonsgegevens niet langer zal zijn dan noodzakelijk voor het doel van de verwerking ten behoeve waarvan de persoonsgegevens worden verwerkt. Overeenkomstig deze instructie handelt de opdrachtnemer.

Artikel 3 - Vernietiging van persoonsgegevens

1. Op verzoek van de opdrachtgever worden bij beëindiging van de onderliggende dienstenovereenkomst de persoonsgegevens ter beschikking gesteld aan de opdrachtgever.
2. Indien er geen verzoek wordt gedaan bij beëindiging van de onderliggende dienstenovereenkomst om de gegevens terug te ontvangen, verwijdert de opdrachtnemer de gegevens direct na beëindiging van de dienstenovereenkomst.

3. Op verzoek van de opdrachtgever verwijdert de opdrachtnemer alle persoonsgegevens definitief welke in opdracht van de opdrachtgever zijn verwerkt, tenzij de opdrachtnemer wettelijk verplicht is tot opslag van deze persoonsgegevens.
4. De opdrachtnemer verwijdert geen persoonsgegevens welke als bewijs kunnen dienen dat de opdrachtnemer heeft voldaan aan haar contractuele afspraken met de opdrachtgever.
5. De opdrachtnemer draagt er zorg voor dat aan de subverwerkers doorgegeven wordt dat de onderliggende dienstenovereenkomst en daarmee de rechtsgrondslag voor de gegevensverwerking is komen te vervallen.

Artikel 4 - Subverwerkers

1. De opdrachtnemer is gerechtigd bij de uitvoering van haar dienst gebruik te maken van subverwerkers.
2. De opdrachtnemer licht de opdrachtgever in over beoogde veranderingen betreffende de toevoeging of vervanging van andere verwerkers.
3. De opdrachtgever heeft het recht tegen de toevoeging of vervanging van een subverwerker bezwaar maken.
4. De opdrachtnemer sluit met subverwerkers een verwerkersovereenkomst onder zodanige voorwaarden dat zij kan voldoen aan de voorwaarden welke zijn vastgelegd in deze verwerkersovereenkomst met de opdrachtgever.
5. In bijlage “Subverwerkers” is een overzicht opgenomen van verwerkers waar de opdrachtnemer gebruik van maakt bij de uitvoering van haar dienst. Desgevraagd zal de opdrachtnemer inzage geven in verwerkersovereenkomsten welke gesloten zijn met deze subverwerkers.

Artikel 5 - Gerelateerde verwerkers

1. Uitsluitend in opdracht van de opdrachtgever integreert de opdrachtnemer diensten/producten van andere verwerkers in haar eigen dienst.
2. De opdrachtgever bepaalt welke diensten/producten dat zijn en is zelf verantwoordelijk voor het sluiten van verwerkersovereenkomsten met deze andere verwerkers.
3. In bijlage “Gerelateerd verwerkers” is een overzicht opgenomen van verwerkers, waarvan de opdrachtnemer software producten/diensten integreert in opdracht van de opdrachtgever.

Artikel 6 - Verwerkingen buiten de Europese Unie

1. De opdrachtnemer verklaart in beginsel alleen persoonsgegevens te verwerken binnen de EU.
2. Indien persoonsgegevens buiten de EU worden verwerkt geschiedt dit met schriftelijke toestemming van de opdrachtgever.

3. Verwerkingen buiten de EU geschiedt alleen in landen die passende waarborgen bieden en waar betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken of waar een adequaatheidsbesluit door de Europese Commissie voor is afgegeven.

Artikel 7 - Aansprakelijkheid

1. De aansprakelijkheid van de opdrachtnemer beperkt zich tot directe schade, als gevolg van nalatig handelen door de opdrachtnemer.
2. Ontstane schade kan niet op de opdrachtnemer verhaalt worden indien de opdrachtnemer heeft voldaan aan alle door de opdrachtgever gestelde voorwaarden.
3. De opdrachtnemer kan niet aansprakelijk worden gehouden indien de opdrachtgever niet tijdig en correct de door de opdrachtnemer aanbevolen technische en organisatorische maatregelen heeft getroffen en daaruit schade is ontstaan.
4. Indien in het overige geval de betrokkene voor haar ontstane schade bij de opdrachtnemer een claim indient waarvan de oorzaak niet het gevolg is van nalatig handelen van de opdrachtnemer, wordt het door de opdrachtnemer uitgekeerde door de opdrachtgever aan de opdrachtnemer gecompenseerd.

Artikel 8 - Vrijwaring

De opdrachtgever vrijwaart de opdrachtnemer voor alle aanspraken van derden met betrekking tot de verwerking van persoonsgegevens.

Artikel 9 - Beveiliging van persoonsgegevens

1. De opdrachtnemer neemt zowel technische als organisatorische maatregelen om de veiligheid te waarborgen en te voorkomen dat de verwerking inbreuk maakt op de Algemene verordening gegevensbescherming.
2. De genomen maatregelen waarborgen een passend niveau van beveiliging, met inbegrip van vertrouwelijkheid, daarbij wordt rekening gehouden met de stand van de techniek en de uitvoeringskosten afgezet tegen de risico's en de aard van de te beschermen persoonsgegevens.
3. Onder risico’s wordt verstaan risico’s op de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot de doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk, hetzij onrechtmatig.
4. De opdrachtnemer treft passende maatregelen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van de opdrachtnemer en toegang heeft tot persoonsgegevens, deze slechts in opdracht van de de opdrachtgever verwerkt, tenzij hij wettelijk anders verplicht is.
5. In bijlage “Technische en organisatorische maatregelen” is een overzicht opgenomen met concrete technische en organisatorische maatregelen welke in ieder geval ter beveiliging van persoonsgegevens zijn genomen.

Artikel 10 - Controle op gegevensverwerking

1. De opdrachtgever heeft het recht eens per jaar een audit, waaronder inspectie, door de opdrachtgever of een door de opdrachtgever gemachtigde controleur uit te voeren.
2. De opdrachtnemer stelt alle informatie ter beschikking aan de opdrachtgever die nodig is om de nakoming van de in deze verwerkersovereenkomst neergelegde verplichtingen aan te tonen.
3. De opdrachtgever heeft het recht om de opdrachtnemer eenmaal per jaar op locatie te controleren op de uitvoering van de gemaakte afspraken welke betrekking hebben op de gegevensverwerking door de opdrachtnemer in opdracht van de opdrachtgever. De werkzaamheden van de opdrachtnemer mogen daarbij niet onnodig worden verstoord.
4. Interne, personele kosten, zijn voor zover redelijk voor rekening van de opdrachtnemer, eventuele ingeschakelde onafhankelijke auditors zijn, voor rekening van de opdrachtgever.
5. Indien uit de audit blijkt dat de opdrachtnemer niet de gemaakte afspraken nakomt zal deze, binnen een nader vast te stellen periode, deze tekortkoming herstellen.
6. De opdrachtgever zal de opdrachtnemer 30 dagen van te voren aankondigen dat een controle zal plaatsvinden. Bij de controle-aankondiging zal worden aangegeven op welke wijze de controle zal plaatsvinden.

Artikel 11 - Meldplicht en documentatieplicht

1. Zodra de opdrachtnemer ervan kennis heeft genomen dat een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, zal de opdrachtnemer de opdrachtgever daarvan direct en zonder onredelijke vertraging op de hoogte stellen, zodat de opdrachtgever indien nodig de autoriteiten en/of de betrokkenen daarvan op de hoogte kan stellen.
2. Indien de opdrachtnemer de opdrachtgever op de hoogte stelt van een inbreuk in verband met persoonsgegevens meldt de opdrachtnemer de feiten omtrent de inbreuk in verband met persoonsgegevens, een schatting van het aantal getroffen betrokkenen, de waarschijnlijke gevolgen daarvan en de genomen corrigerende maatregelen om de inbreuk te stoppen en de nadelige gevolgen te beperken.
3. De opdrachtnemer houdt van iedere inbreuk documentatie bij inclusief de daarbij behorende specificaties als genoemd in het voorgaande lid.

Artikel 12 - Vertrouwelijkheid van persoonsgegevens

1. De opdrachtnemer zorgt ervoor dat haar personeel en andere gemachtigden contractueel verplicht zijn om vertrouwelijk om te gaan met de persoonsgegevens die zij verwerken. Op verzoek kan de opdrachtnemer hiervan schriftelijk bewijs overleggen.
2. Het personeel van de opdrachtnemer zal geen persoonsgegevens doorspelen of uitlatingen betreffende de persoonsgegevens doen, aan anderen zonder toestemming van de opdrachtgever, tenzij de opdrachtnemer daar wettelijk toe verplicht is. In dat geval stelt de

opdrachtnemer de opdrachtgever, voorafgaand aan de verwerking, in kennis van de bepaling die ten grondslag ligt aan deze verplichting.

3. Indien de opdrachtnemer een wettelijk bevel ontvangt om persoonsgegevens ter beschikking te stellen aan de daartoe bevoegde autoriteiten, zal de opdrachtnemer direct de opdrachtgever daarvan op de hoogte stellen, tenzij dat wettelijk verboden is.
4. De opdrachtnemer zorgt ervoor dat de verplichting tot vertrouwelijke omgang van persoonsgegevens door personeel en overige gemachtigde personen, vanwege haar aard, doorwerkt na de beëindiging van het arbeidscontract.
5. De opdrachtnemer draagt er zorg voor dat deze vertrouwelijkheidsverplichting eveneens in de contracten met haar subverwerkers is opgenomen.

Artikel 13 - Controle en correctie-rechten van betrokkenen

1. De opdrachtnemer zal, voor zover als redelijk, bijstand verlenen aan de opdrachtgever bij het uitoefenen van diens plicht om verzoeken van betrokkenen bij de uitoefening van hun rechten als bedoeld in de Algemene verordening gegevensbescherming te beantwoorden.
2. De opdrachtnemer zal, voor zover als redelijk, passende en technische maatregelen nemen om aan deze verzoeken gehoor te kunnen geven.

Artikel 14 - Toepasselijkheid van de verwerkersovereenkomst

1. Deze verwerkersovereenkomst houdt op te bestaan zodra de dienstenovereenkomst tussen de de opdrachtgever en de opdrachtnemer is beëindigd.
2. Bepalingen welke naar hun aard dienen voort te bestaan blijven ook na beëindiging van de dienstenovereenkomst van kracht.
3. De bepalingen in deze verwerkersovereenkomst prevaleren boven iedere andere gemaakte afspraak tussen de opdrachtgever en opdrachtnemer, voor wat betreft de verwerking van persoonsgegevens.
4. Indien door wijzigende omstandigheden of inzichten de voorwaarden van deze verwerkersovereenkomst dienen te wijzigen zullen partijen in samenspraak hiertoe overgaan.
5. Op deze verwerkersovereenkomst is naast de Algemene verordening gegevensbescherming, alleen Nederlands recht van toepassing.
6. Geschillen die ontstaan naar aanleiding van deze verwerkersovereenkomst worden voorgelegd aan de bevoegde rechter in het arrondissement waarin de opdrachtnemer gevestigd is.

Datum: Datum:

Handtekening opdrachtgever: Handtekening opdrachtnemer:

Voorbeeld Verwerkersovereenkomst “Doelen en middelen”

(Behorende bij artikel 1 lid 3)

Uitvoering van de overeenkomst

De gegevens die de betrokkene heeft aangeleverd bij het aangaan van de producten en/of diensten worden gebruikt voor het uitvoeren van de betreffende overeenkomst.

Formulieren

De gegevens welke worden ingevuld door de betrokkene in formulieren worden uitsluitend gebruikt voor het doel welke het formulier dient. Dit kunnen onder andere zijn klachtenformulier, contactformulier, boekingsformulier, klanttevredenheidsenquêtes, aanmeldformulieren. Het IP adres van de betrokkene wordt bij ieder verstuurd en opgeslagen formulier verwerkt ter beveiliging van de website.

Marketing

Voor het versturen van online aanbiedingen, nieuwsbrieven en magazines worden alleen de gegevens verwerkt die noodzakelijk zijn voor het versturen daarvan. Wanneer de betrokkene zich afmeldt voor online marketing worden gegevens terstond uit de mailinglijst verwijderd.

Backup

De backup van persoonsgegevens worden niet langer opgeslagen dan nodig ten behoeve van herstelmogelijkheden.

Voorbeeld Verwerkersovereenkomst "Gerelateerde verwerkers" (Behorende bij artikel 5 lid 3)

De opdrachtnemer integreert in opdracht van de opdrachtgever, diensten/producten van andere verwerkers. De opdrachtgever is zelf verantwoordelijk voor het sluiten van een verwerkersovereenkomst met deze partijen.

Google Analytics & Google Tag Manager
Google Analytics wordt standaard geïmplementeerd zodat het IP adres wordt geanonimiseerd en de gegevens alleen anoniem gedeeld worden.

Tracking
In de website worden tracking pixels geïmplementeerd om bezoeken te registreren en deze bezoekers op andere platformen gerichte informatie aan te bieden.

Voorbeeld Verwerkersovereenkomst “Subverwerkers”

(Behorende bij artikel 4 lid 5)

De opdrachtnemer maakt ten behoeve van de uitvoering van haar dienst, in hoedanigheid van verwerker, gebruik van subverwerkers. De opdrachtnemer heeft met deze partijen een verwerkersovereenkomst gesloten onder zodanige voorwaarden dat de opdrachtnemer aan haar verplichtingen gesteld in deze verwerkersovereenkomst kan voldoen.

NAAM Hostingbedrijf

NAAM Hostingbedrijf biedt servercapaciteit, bandbreedte, domeinnamen, SSL certificaten, backup faciliteiten, monitoring en onderhoud.

Voorbeeld Verwerkersovereenkomst “Technische en organisatorische maatregelen” (Behorende bij artikel 9 lid 5)

Opdrachtnemer neemt in ieder geval onderstaande technische en organisatorische maatregelen ter beveiliging van de persoonsgegevens Wachtwoordbeleid Wachtwoorden worden voor automatisch gegenereerd middels een wachtwoordmanager. Deze worden gehasht in een middels wachtwoord beveiligde database opgeslagen. De pogingen worden gelogd en beperkt. Versleuteling van gegevens Persoonsgegevens worden versleuteld verstuurd, waarbij gebruik gemaakt wordt van publieke sleutel certificaten afgegeven door een certificeringsautoriteit. Deze sleutels hebben een beperkte duur.

Systeembeveiliging Gegevensopslag
De gegevensopslag welke persoonsgegevens bevatten zijn beveiligd met wachtwoorden die automatisch en willekeurig gegenereerd worden.

Netwerk
Een specifieke functionaris is aangewezen om intern de rechten tot het netwerk te beheren. Rechten worden volgens een bepaalde procedure toegewezen en afgenomen. Het gebruik van het netwerk wordt gemonitord en gelogd. Voor het beveiligd versturen van persoonsgegevens wordt gebruik gemaakt van SSL verbindingen.

Personeel
Contractueel is overeengekomen dat personeel vertrouwelijk dient om te gaan met de persoonsgegevens. Deze verplichting werkt door tot na beëindiging van het dienstverband. In de huisregels van de opdrachtnemer, welke gepubliceerd zijn op het intranet, worden medewerkers met specifieke gedragsvoorschriften geïnstrueerd zorgvuldig om te gaan met persoonsgegevens.

Subverwerkers
Met subverwerkers genoemd in Bijlage 3 zijn verwerkersovereenkomsten gesloten onder zodanige voorwaarden dat opdrachtnemer aan haar verplichtingen voortvloeiende uit deze overeenkomst kan voldoen.

Overzicht
De opdrachtnemer heeft inzichtelijk welke persoonsgegevens zich in welke, voor de opdrachtnemer toegankelijke systemen bevinden. In beginsel is de opdrachtnemer in staat terstond, maar uiterlijk binnen 5 werkdagen mutaties te doen op de persoonsgegevens.

Bijlage 5 - Cameratoezicht in winkels, horeca en sportclubs

Cameratoezicht in of rond een winkel, horecagelegenheid of sportclub kan helpen om eigendommen, bezoekers en personeel te beschermen. Maar de inbreuk op de privacy van klanten en werknemers is groot. Daarom mogen ondernemers alleen camera's ophangen als zij aan een aantal voorwaarden voldoen. Ook moeten zij ervoor zorgen dat de inbreuk op de privacy van de klanten en het personeel zo klein mogelijk is. Een camera in een pashokje, kleedkamer of toilet gaat te ver, omdat mensen dan ontkleed in beeld kunnen komen.

Gerechtvaardigd belang
De ondernemer moet een zogeheten gerechtvaardigd belang hebben voor het cameratoezicht. Bijvoorbeeld diefstal tegengaan of klanten en werknemers beschermen.

Noodzaak cameratoezicht
Het cameratoezicht moet noodzakelijk zijn. Dat wil zeggen dat de ondernemer het doel niet op een andere manier kan bereiken. Is er geen andere mogelijkheid, die minder ingrijpend is voor de privacy? Dat moet de ondernemer eerst nagaan.

Ook mag het cameratoezicht niet op zichzelf staan. Het moet onderdeel zijn van een totaalpakket aan maatregelen.

Privacytoets
De ondernemer moet eerst een privacytoets uitvoeren. Dit betekent dat hij de belangen van de klanten en de werknemers afweegt tegen zijn eigen belang.

Informatieplicht cameratoezicht
Voordat klanten naar binnen gaan, moeten zij kunnen weten dat er cameratoezicht is. De ondernemer moet dit laten weten. Bijvoorbeeld door bordjes op te hangen.

Bewaartermijn camerabeelden
De ondernemer mag de camerabeelden niet langer bewaren dan noodzakelijk is. De richtlijn hiervoor is maximaal 4 weken.

Maar is er een incident vastgelegd, zoals diefstal? Dan mag de ondernemer de betreffende beelden bewaren tot dit is afgehandeld.

Zie ook:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/dos_en_donts_cameratoezicht_autoriteit_persoonsgegevens.pdf

Bijlage 6 – Interessante links

https://rvo.regelhulpenvoorbedrijven.nl/avg/welkom

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/2017-11_stappenplan_avg_online_v2.pdf

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/2017-11_stappenplan_avg_online_v2.pdf

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/avg_in_een_notendop.pdf

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleidingalgemeneverordeninggegevensbescherming.pdf

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg#publications