|  |  |
| --- | --- |
|  | Functioneel Ontwerp |
|  |  |
| 11/10/2018 | Biker |
|  | Door: Rick Wubs (626010), Leroy Wijnands (622311), Mike Beskers (620379) Klas: BIS DT C Docent: Drs. Ing. G. Heijink |

Biker

# Inhoudsopgave

[1 Inhoudsopgave 1](#_Toc526939882)

[2 Inleiding 3](#_Toc526939883)

[2.1 Aanleiding 3](#_Toc526939884)

[2.2 Doelstelling 3](#_Toc526939885)

[3 Procesmodellen 4](#_Toc526939886)

[4 Requirements 8](#_Toc526939887)

[4.1 Business requirements 8](#_Toc526939888)

[4.2 User requirements 8](#_Toc526939889)

[4.3 NIET FUNCTIONELE REQUIREMENTS 10](#_Toc526939890)

[5 USE CASE DIAGRAM 11](#_Toc526939891)

[5.1 Use Case beschrijvingen (High Level) 12](#_Toc526939892)

[5.2 Full dressed use cases 15](#_Toc526939893)

[6 Use case diagram 18](#_Toc526939894)

[7 Wireframes 18](#_Toc526939895)

[8 Maatregelen gegevensbescherming 18](#_Toc526939896)

[8.1 Uitgangspunten informatiebeveiliging “Biker” 18](#_Toc526939897)

[8.1.1 Het belang van informatie 18](#_Toc526939898)

[8.1.2 Visie 18](#_Toc526939899)

[8.1.3 Doelstelling 18](#_Toc526939900)

[8.1.4 Uitgangspunten 18](#_Toc526939901)

[8.1.5 Risicobenadering 18](#_Toc526939902)

[8.1.6 Doelgroepen 19](#_Toc526939903)

[8.1.7 Scope 19](#_Toc526939904)

[8.1.8 IB-beleid en architectuur 19](#_Toc526939905)

[8.1.9 Werking 19](#_Toc526939906)

[8.2 Organisatie van de informatiebeveiliging 19](#_Toc526939907)

[8.2.1 Interne organisatie 19](#_Toc526939908)

[8.2.2 Taken en rollen 20](#_Toc526939909)

[8.2.3 Functioneel overleg 21](#_Toc526939910)

[8.2.4 Rapportage en escalatielijn voor IB 21](#_Toc526939911)

[8.3 Beheer van bedrijfsmiddelen 21](#_Toc526939912)

[8.3.1 Verantwoordelijkheid voor bedrijfsmiddelen 21](#_Toc526939913)

[8.3.2 Classificatie van informatie 22](#_Toc526939914)

[8.4 Beveiliging van personeel 24](#_Toc526939915)

[8.4.1 Risico’s 24](#_Toc526939916)

[8.4.2 Doelstelling 24](#_Toc526939917)

[8.4.3 Beheersmaatregelen 24](#_Toc526939918)

[8.4.4 Bewustwording 25](#_Toc526939919)

[8.5 Fysieke beveiliging en beveiliging van de omgeving 25](#_Toc526939920)

[8.5.1 Risico’s 25](#_Toc526939921)

[8.6 Beveiliging van apparatuur en informatie 25](#_Toc526939922)

[8.6.2 Beheersmaatregelen 26](#_Toc526939923)

[8.6.3 Beheer van de dienstverlening door een derde partij 27](#_Toc526939924)

[8.6.4 Behandeling van media 28](#_Toc526939925)

[8.6.5 Uitwisseling van informatie 28](#_Toc526939926)

[8.7 Logische toegangsbeveiliging 29](#_Toc526939927)

[8.7.1 Authenticatie en autorisatie 29](#_Toc526939928)

[8.7.2 Mobiel en thuiswerken 29](#_Toc526939929)

[8.7.3 Overige maatregelen 29](#_Toc526939930)

[8.7.4 Beveiliging van informatiesystemen (software) 29](#_Toc526939931)

[8.8 Beveiligingsincidenten 30](#_Toc526939932)

[8.8.1 Melding en registratie 30](#_Toc526939933)

[8.9 Bedrijfscontinuïteit 30](#_Toc526939934)

[8.9.1 Risico’s 30](#_Toc526939935)

[8.9.2 Doelstelling 30](#_Toc526939936)

[8.10 Naleving 30](#_Toc526939937)

[8.10.1 (Wettelijke) kaders 30](#_Toc526939938)

[9 Bijlage 1: Relevante bepalingen avg 31](#_Toc526939939)

# Inleiding

## Aanleiding

Biker is een fietsverhuur bedrijf in de regio Arnhem/Nijmegen. Dit functioneel ontwerp richt zich op de vestiging te Nijmegen. Klanten kunnen online of aan de balie fietsen huren, al dan niet in combinatie met accessoires en keuze uit een tweetal reizen. Doel is om de processen zo goed mogelijk te organiseren. Ten einde van dit doel worden een aantal processen in een elektronisch systeem ondergebracht. Het betreft de planning van medewerkers, het aanbieden van fietsenverhuur met bijbehorende opties via de website, het voorraadbeheer, het betaalproces en de administratie van retournatie en reparatie.

## Doelstelling

Aan ons is de vraag gesteld om hiervoor een functioneel ontwerp op te stellen voor Biker. Het functioneel ontwerp is opgesteld aan de hand van de casusbeschrijving. De processen zijn beschreven (hoofdstuk 2). Na het beschrijven van de processen zijn de requirements opgesteld (zie hoofdstuk 3).

**De inleiding is niet volledig. Deze moet worden uitgebreid en aangevuld door de studenten.**

**De dik gedrukte tekst is een toelichting of aandachtspunt voor de student. Deze hoeft niet perse in het functioneel ontwerp opgenomen te worden. Soms is het duidelijk om gemaakte keuzes toe te lichten.**

# Procesmodellen

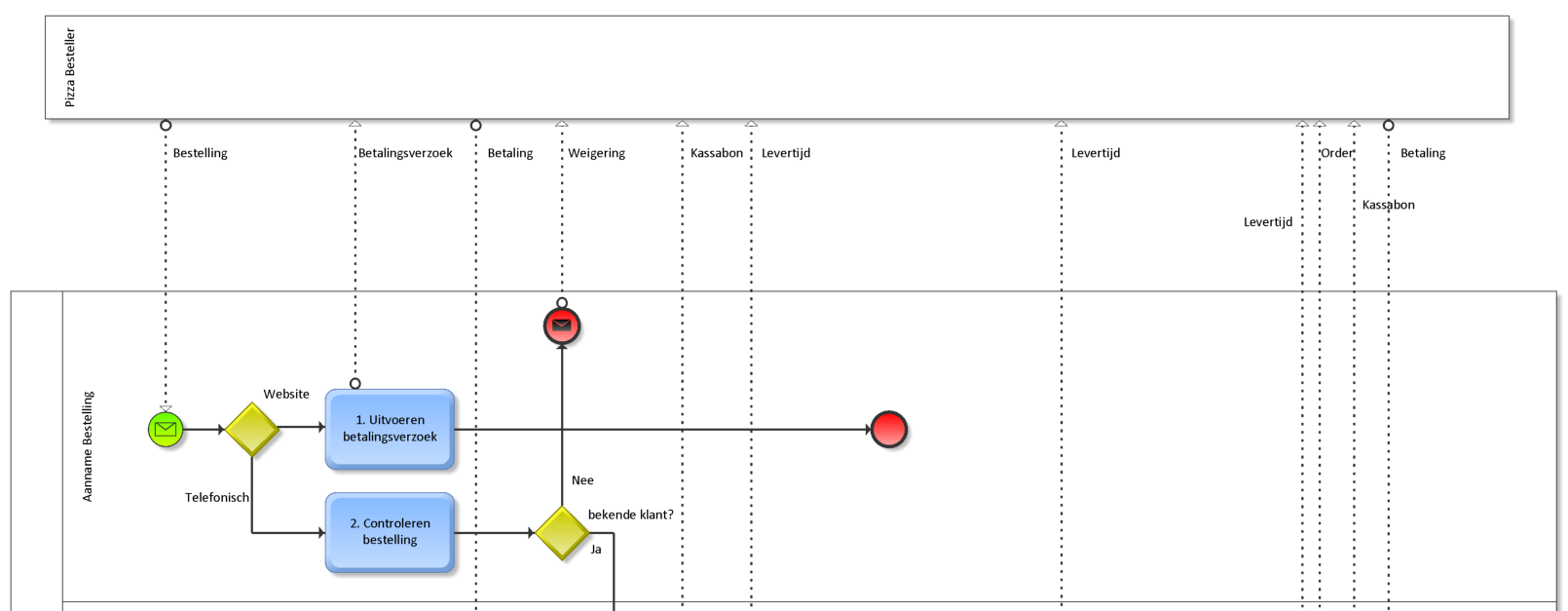
De processen zijn in dit hoofdstuk zijn beschreven met behulp van de BPMN-notatie. In figuur 1 zijn de globale processen uitgewerkt. Deze zijn hierna apart in meer detail uitgewerkt. Deze keuze is tot stand gekomen door het gedetailleerd willen beschrijven van de processen, zonder hierbij het overzicht te verliezen. De documentatie van de processen zijn in de respectievelijke tabellen opgenomen.

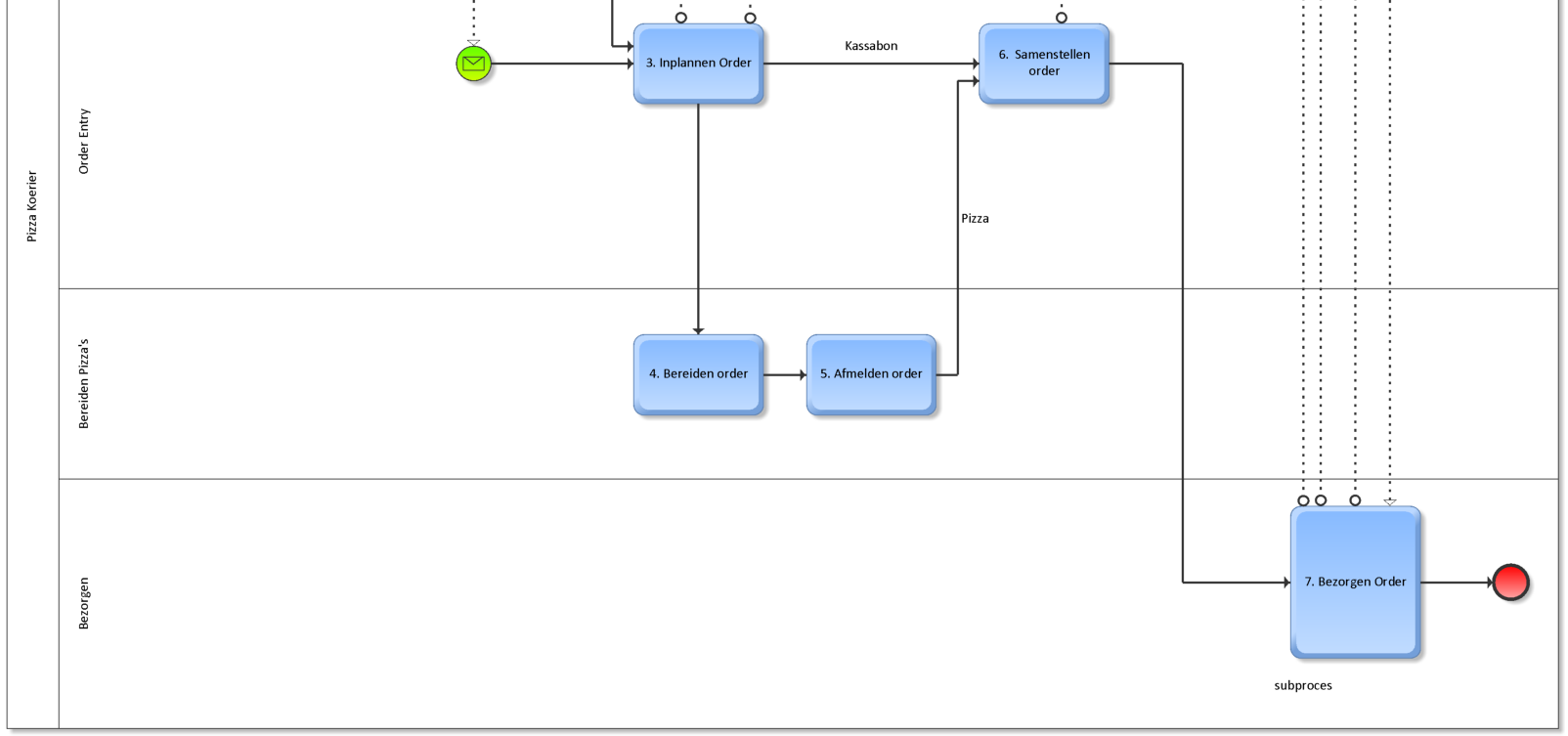
**Toelichting:**De klant is als een white-box pool getekend. Hou echter in de gaten dat de Klant ook de volgende (niet in het proces gemodelleerde) bewerkingen moet kunnen uitvoeren:

- een selectie moet kunnen maken uit het aanbod van verschillende pizza’s;  
- een betaling moet kunnen uitvoeren;  
- zijn klantgegevens moet kunnen actualiseren/registreren (om telefonisch te kunnen bestellen).

Alleen telefonische bestellingen worden gecontroleerd (postcodehuisnummer en geboortedatum). Voor de andere bestellingen geldt dat altijd een betalingsverzoek wordt aangemaakt.

Het subproces “Bezorgen Order” is als child-level expansion in een apart diagram (figuur 2) getekend.

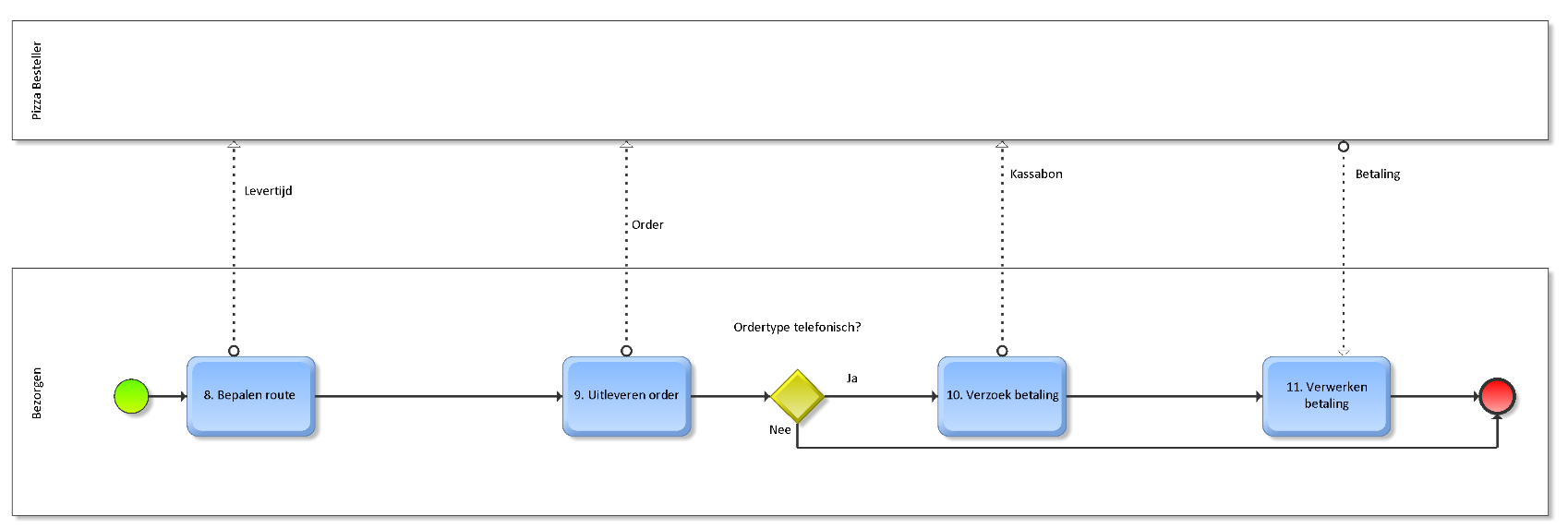
Figuur 1. PIZZA KOERIER  




Tabel 1. Documentatie Biker

|  |  |  |
| --- | --- | --- |
| Invoer | Werking | Uitvoer |
| Bestelling via website of balie | *1. Uitvoeren betalingsverzoek (service task)*  In ontvangst nemen van de bestelling en berekenen bestel bedrag. | Betalingsverzoek |
| Bestelling via balie | *2. Uitvoeren betalingsverzoek (service task)*  In ontvangst nemen van de bestelling en berekenen bestel bedrag. | Betalingsverzoek |
| Betaling | *3. Inplannen order (service task)*  Omzetten van een “Betaling” (die betrekking heeft op een bestelling) naar een Order.  Op basis van Order levertijd bepalen. | Kassabon Levertijd |
| Order | *4. Klaarzetten order (user task)*  Klaarzetten van benodigde fietsen, accessoires op basis van Order | Fiets |
| Fiets | *5. Afmelden order (user task)*  Verstrekken Order aan baliemedewerker. | Fiets |
| Kassabon Fiets | *6 Samenstellen order (user task)*  Groeperen Orders tot één Uitlevering.  Kassabon toevoegen aan Order.  Voorraadbeheer bijwerken. | Uitlevering Kassabon Voorraad |
| Kassabon of identificatie  Fiets | *7. Retournatie (subproces)*  Controleren retournatie.  Opstellen prijsbepaling reparatiekosten.  Bijwerken voorraadbeheer. | Kassabon  Fiets  Voorraad |

Figuur 2. Bezorgen Order



Tabel 2. Documentatie biker

|  |  |  |
| --- | --- | --- |
| Invoer | Werking | Uitvoer |
| Uitlevering | *9. Uitleveren order (user task)*  Verstrekken order. | Order  Kassabon |
| Kassabon | *10. Verzoek betaling (user task)*  Betalingsverzoek (op basis kassabon). | Kassabon |
| Betaling | *11. verwerken betaling (user task)*  Ontvangen betaling. |  |

# Requirements

**Korte inleiding opnemen.**

## Business requirements

De eigenaar wil het verhuren van fietsen online aanbieden in combinatie met accessoires en reisverhuur.

De eigenaar wil de klanttevredenheid verhogen van **X** naar **X** procent.

De eigenaar wil de omzet in 2018 verhogen met **X** procent.

## User requirements

De user requirements zijn opgenomen in tabel 2 als user stories.

Tabel 3. User Requirements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nummer** | **User Story(s) = Requirement** | | | **Prioriteit** |
|  | **Als een <type gebruiker>** | **Wil ik <iets doen>** | **Zodat ik <er iets aan heb>** |  |
| UC-B1 | Klant | Wil ik fietsen bestellen via internet | Zodat ik zeker weet dat deze beschikbaar zijn. | Must |
| UC-B2 | Klant | Wil ik accessoires aan mijn bestelling kunnen toevoegen | Zodat ik alle benodigdheden op een plek kan bestellen. | Must |
| UC-B3 | Klant | Wil ik mijn geboortedatum, naam, adres, woonplaats, telefoonnummer en email adres kunnen opgeven | Zodat ik kan bestellen | Must |
| UC-B4 | Klant | Wil ik reizen kunnen boeken | Zodat ik alle benodigdheden op een plek kan bestellen. | Should |
| UC-B5 | Klant | Wil ik een bevestigingsbericht ontvangen van de order | Zodat ik weet dat mijn bestelling inderdaad voorradig is. | Should |
| UC-B6 | Baliemedewerker | Wil ik dat de klanten wanneer zij via internet een bestelling doen direct de bestelling betalen | Zodat ik zeker weet dat het een serieuze bestelling is en ik niet opgelicht word. | Must |
| UC-B7 | Baliemedewerker | Wil ik alleen fietsen kunnen bestellen die ook voorradig zijn. | Zodat ik zeker weet dat ze geleverd kunnen worden. | Must |
| UC-B8 | Baliemedewerker | Wil ik dat ik alleen bestellingen in ontvangst neem die betaald zijn of waarvan de klant een bekende klant is. | Zodat ik geen financieel risico loop | Must |
| UC-B9 | Reparateur | Wil ik kunnen aangeven wat de voorraad is | Zodat er geen fietsen worden afgegeven die we niet voorradig hebben | Must |
| UC-B10 | Reparateur | Wil ik fietsen kunnen aanmelden | Zodat we weten wat we op voorraad hebben | Must |
| UC-B11 | Reparateur | Wil ik retournatie als compleet kunnen aanmelden | Zodat we weten dat de klant alles correct terug heeft geleverd | Must |
| UC-B12 | Reparateur | Wil ik fietsen als ‘in reparatie’ kunnen aanmelden | Zodat we weten hoeveel voorraad tijdelijk niet beschikbaar is | Should |
| UC-B13 | Planner | Wil ik kunnen zien wat de vrije dagen van de medewerkers zijn | Zodat ik ze niet inplan op dagen dat ze niet kunnen werken | Must |
| UC-B14 | Planner | Wil ik een overzicht van de orders kunnen zien | Zodat ik op drukke dagen op locatie extra mensen in kan plannen | Should |

## NIET FUNCTIONELE REQUIREMENTS

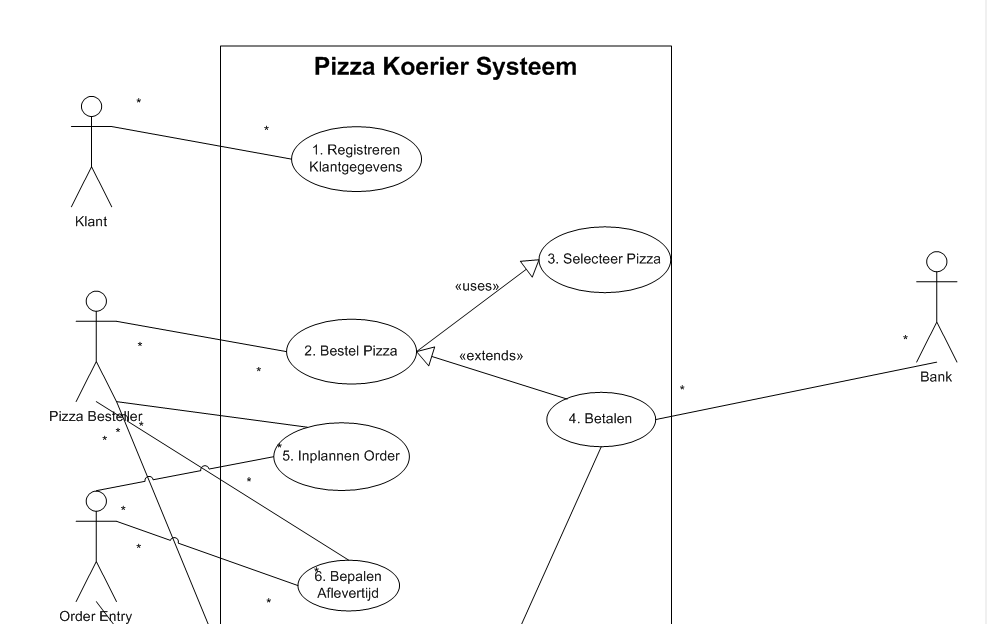
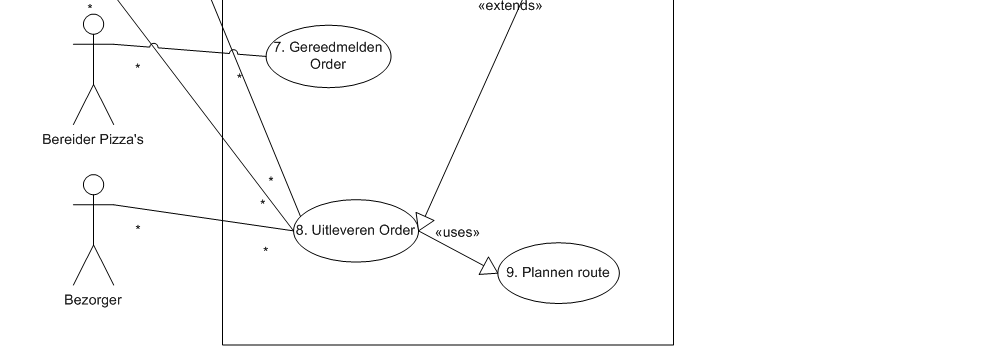
**Introductie opnemen.**

1. (U) De voorpagina moet duidelijk de aanbiedingen tonen;
2. (U) Er moet een menu-item komen die linkt naar een overzicht van alle fietsen;
3. (U) Elke schermwisseling mag maximaal één seconde duren;
4. (U) De afhandeling van een transactie mag niet langer dan twee seconden duren;
5. (U) Er moet een menu-item komen die linkt naar een overzicht van alle reizen;
6. (R) De beschikbaarheid van het systeem moet 99,8% per dag zijn;
7. (R) Het systeem mag maximaal **X** minuten offline zijn bij updates;
8. (R) Het systeem mag maximaal **X** minuten offline zijn bij hardware corruptie;
9. (R) Er moet een failover server zijn waarop de processen door draaien bij hardware fouten;
10. (R) Er dient IP-filtering plaats te vinden om het risico van DDOS te minimaliseren;
11. (P) Het systeem moet tot 1000 gebruikers tegelijk aan kunnen;
12. (P) Het systeem moet binnen **X**-milliseconden de pagina gepaint hebben;
13. (P) Het systeem moet uit te breiden zijn om meer gebruikers tegelijk aan te kunnen;
14. (P) Uitbreidingen dienen niet ten koste te gaan van de laadsnelheid van de pagina’s;
15. (P) Het systeem mag maximaal **X%** RAM en CPU gebruiken;
16. (S) Foutmeldingen dienen binnen **X** minuten te zijn opgelost;
17. (S) Het systeem dient modulair uit te breiden te zijn;
18. (S) Er moet duidelijke documentatie zijn over de werking van het systeem;
19. (S) Eventuele errors dienen binnen **X** minuten gehotfixed te worden;
20. (S) Codewijzigingen dienen duidelijk gedocumenteerd te worden;

# USE CASE DIAGRAM

**Korte inleiding opnemen.**

Het use case diagram staat afgebeeld in figuur 2. De actoren zijn beschreven in tabel 3. Een beschrijving van de use cases is opgenomen in hoofdstuk 5.1.

Figuur 2 Use Case diagram pizza koerier SYSTEEM

**Toelichting op het use case diagram:**

1. Betalen is als Extend gemodelleerd bij Bestellen Pizza en Uitleveren Order.   
   Pas als er betaald is wordt een order aangemaakt (order = bestelling + betaling).
2. Alleen telefonische bestellingen moeten bij uitleveren worden betaald.
3. Onderhouden klantgegevens is als aparte use case gemodelleerd omdat de eigenaar klanten met een account in de toekomst voordelen wilt gaan bieden. Klantgegevens worden dan onderhouden.
4. Betalen moet eigenlijk nog verder uitgewerkt worden als generalisatie. Hoe doe je dat?
5. Is het noodzakelijk om “Bereiden Pizza” als use case op te nemen (met als actor Bereiden Pizza’s)?

Tabel 4. Beschrijving van de actoren

|  |  |  |
| --- | --- | --- |
| Actor | Toelichting | Primair / Secundair |
| Klant | Iemand die zich kan registreren. Na registratie (en controle daarvan) kan hij bestellingen verrichten. | Primair |
| Pizza Besteller | Persoon die een bestelling plaatst. | Primair |
| Order Entry | Omzetten van bestellingen naar ingeplande orders. | Primair |
| Bereiden Pizza’s | Gereedmelden van bereide orders | Primair |
| Bezorgen | Uitleveren van orders en in ontvangst nemen van betalingen | Primair |
| Bank | Verwerken van betalingen | Secundair |

## Use Case beschrijvingen (High Level)

In dit hoofdstuk worden alle use cases zoals staan afgebeeld in het use case diagram (high level) beschreven. Voor elke use case is beschreven:

1. De naam van de use case  
2. De requirements(s) waaraan de use case invulling geeft (zie tabel2: user requirements)  
3. De actor(en) (zie tabel3: beschrijving van de actoren)  
4. De purpose (wat is het doel van de use case, waarom existeert de use case?)  
5. Het gedrag dat de use case vertoont in de vorm van de userstory (zie tabel2: user

requirements).

|  |  |
| --- | --- |
| Naam | **1 Registeren Klantgegevens** |
| Requirements | 2 |
| Actor(en) | Klant |
| Purpose | Het voor een Klant mogelijk maken om pizza’s te bestellen |
| Overview/Scenario’s | Als klant wil ik mijn geboortedatum, naam, adres, woonplaats, telefoonnummer en email adres kunnen opgeven zodat ik kan bestellen. |

|  |  |
| --- | --- |
| Naam | **2 Bestel Pizza** |
| Requirements | 1 |
| Actor(en) | Pizza Besteller |
| Purpose | Het voor een Klant mogelijk maken om een bestelling te plaatsen |
| Overview/Scenario’s | Als Pizza Besteller wil ik pizza’s bestellen via internet zodat ik lekker thuis, vanuit m’n luie stoel kan bestellen en het huis niet uit hoef. |

|  |  |
| --- | --- |
| Naam | **3 Selecteer Pizza** |
| Requirements | 6 |
| Actor(en) | Pizza Besteller |
| Purpose | Inzage geven in de menukaart |
| Overview/Scenario’s | Als Pizza Besteller wil ik alleen pizza’s kunnen bestellen die ook op de menu kaart staan, zodat ik zeker weet dat ze geleverd kunnen worden. |

|  |  |
| --- | --- |
| Naam | **4 Betalen** |
| Requirements | 10 |
| Actor(en) | Pizza Besteller, Bank, Bezorgen |
| Purpose | Afhandelen betaling |
| Overview/Scenario’s | Als Bank wil ik verschillende betaal transacties vlot afhandelen zodat de klant de beschikking krijgt over zijn aankoop |

|  |  |
| --- | --- |
| Naam | **5 Inplannen Order** |
| Requirements | 3, 5, 7, 8 |
| Actor(en) | Order Entry, Pizza Besteller |
| Purpose | Omzetten van bestellingen naar ingeplande orders |
| Overview/Scenario’s | Als Pizza Besteller wil ik een bericht ontvangen van de levertijd van de order zodat ik weet wanneer de order geleverd wordt.  Als Order Entry wil ik dat de klanten wanneer zij via internet een bestelling doen direct de bestelling betalen zodat ik zeker weet dat het een serieuze bestelling is en ik niet opgelicht word.  Als Order Entry wil ik dat ik alleen bestellingen in ontvangst neem die betaald zijn of waarvan de klant een bekende klant is zodat ik geen financieel risico loop  Als Order Entry wil ik orders kunnen inplannen zodat ik een verwachte levertijd aan de klant kan doorgeven. |

|  |  |
| --- | --- |
| Naam | **6 Bepalen Aflevertijd** |
| Requirements | 4 |
| Actor(en) | Pizza Besteller |
| Purpose | Bepalen van de levertijd/aankomsttijd van de order |
| Overview/Scenario’s | Als Pizza Besteller wil ik de status van mijn order volgen zodat ik weet wanneer mijn order geleverd wordt. |

|  |  |
| --- | --- |
| Naam | **7 Gereedmelden Order** |
| Requirements | 11 |
| Actor(en) | Bereiden Pizza’s |
| Purpose | Gereedmelden van een order |
| Overview/Scenario’s | Als Bereiden Pizza’s wil ik order(s) gereedmelden zodat de Pizza Besteller tijdig over zijn eten kan beschikken |

|  |  |
| --- | --- |
| Naam | **8 Uitleveren Order** |
| Requirements | 9, 12 |
| Actor(en) | Bezorgen, Pizza Besteller |
| Purpose | Uitleveren van een order op bezorgadres |
| Overview/Scenario’s | Als Pizza Besteller wil ik dat een pizza thuisbezorgd kan worden zodat ik het huis niet uit hoef  Als Bezorgen Wil ik order(s) kunnen uitleveren zodat de Pizza Besteller tijdig over zijn eten kan beschikken |

|  |  |
| --- | --- |
| Naam | **9 Plannen route** |
| Requirements | 13 |
| Actor(en) | Bezorgen |
| Purpose | Bepalen van de optimale route |
| Overview/Scenario’s | Als Bezorgen wil ik de route van order(s) eenvoudig kunnen plannen zodat de Pizza Besteller tijdig over zijn eten kan beschikken |

## Full dressed use cases

|  |  |  |
| --- | --- | --- |
| Naam | Online bestellen | |
| Actor(s) | Klant, Besteller | |
| Purpose | Het online bestellen van een fiets met bijbehorende accessoires en een reis | |
| Requirements | UC-B1, UC-B2, UC-B3, UC-B4, UC-B5 | |
| Scenario’s | 1. Biker toont de homepagina, welke een overzicht van fietsen toont en een inlog/registratiemogelijkheid biedt. 2. Klant registreert of logt in en wordt hiermee een Besteller. 3. Besteller selecteert een of meerdere fietsen totdat hij tevreden is en naar de pagina ‘accessoires’ gaat. 4. Biker toont de pagina ‘accessoires’, welke een overzicht van de beschikbare accessoires voor de gekozen fietsen staat. 5. Besteller selecteert nul of meer accessoires en geeft aan wanneer hij hiermee klaar is. 6. Biker toont de pagina ‘reizen’, welke een overzicht van de reizen weergeeft. 7. Besteller kiest of hij/zij een reis wil reserveren. 8. Biker toont de pagina ‘kalender’, welke een overzicht van beschikbare data toont waarop de reis genoten kan worden. 9. Besteller kiest de juiste datum voor het begin en eind van de reis. 10. Biker toont de pagina ‘betalen’. 11. Besteller voldoet de online betaling aan Biker. 12. Biker verwerkt de bestelling, verwerkt de betaling en toont de pagina ‘bevestiging’. | |
| WireFrame | De gekoppelde wireframe’s | |
| Preconditie(s) | Klant is op een computer welke verbonden is met het internet | |
| Postconditie(s) | 1. De klant heeft een fiets besteld. 2. De klant heeft een fiets met accessoires besteld. 3. De klant heeft een fiets met reis besteld. 4. De klant heeft een fiets met accessoires en reis besteld. 5. De klant heeft geen bestelling geplaatst. | |
| **Basic Flow (Main Success Scenario)** | | |
| *Actor action* | | *Systems response* |
| Dit proces start wanneer de klant online een fiets (eventueel inclusief accessoires en reis) wil bestellen. | |  |
| 1. Klant navigeert naar de website van Biker. | | 1. Biker toont de homepagina. |
| 1. Klant navigeert naar de inlogpagina. | | 1. Biker toont de inlogpagina. |
| 1. Klant voert de inloggegevens in. | | 1. Klant is ingelogd. 2. Klant wordt hierdoor Besteller. 3. Biker toont de homepagina. |
| 1. Besteller selecteert fietsen totdat hij tevreden is met de fietskeuze. | | 1. Fietsen worden toegevoegd aan de bestelling. |
| 1. Besteller navigeert naar de pagina ‘accessoires’. | | 1. Biker toont de pagina ‘accessoires’, welke een overzicht van de beschikbare accessoires voor de gekozen fietsen geeft. |
| 1. Besteller kiest nul of meer accessoires. | | 1. Accessoires worden toegevoegd aan de bestelling. |
| 1. Besteller navigeert naar de pagina ‘reizen’. | | 1. Biker toont de pagina ‘reizen’. |
| 1. Besteller selecteert de reis naar keuze. | | 1. Biker toont de pagina ‘kalender’. |
| 1. Besteller selecteert de juiste datum voor het begin van de reis. | | 1. Biker voegt de gekozen reis toe aan de bestelling. 2. Biker toont de pagina ‘overzicht’. |
| 1. Besteller controleert de bestelling en navigeert naar ‘betalen’ | | 1. Biker toont de pagina ‘betalen’. |
| 1. Besteller voldoet de online betaling. | | 1. Biker verwerkt de betaling. 2. Biker toont de pagina ‘bevestiging’. |
| De klant heeft nu een bestelling, bestaande uit [één](http://www.dutchgrammar.com/forum/viewtopic.php?t=6832) of meer fietsen, nul of meer accessoires en nul of [één](http://www.dutchgrammar.com/forum/viewtopic.php?t=6832) reis. | |  |
| **Exceptions** | | |
| 3.1 Klant navigeert naar de registratie-pagina. | | 4.1 Biker toont de registratiepagina. |
| 3.2 Klant voert NAW-gegevens in | | 4.2 Biker verwerkt de NAW-gegevens.  4.3 Biker logt de klant in.  4.4 Klant wordt besteller.  4.5 Biker toont de homepagina. |
| 24.1 Klant voldoet de online betaling niet. | | 25.1 Biker verwerkt het betalingsverzoek.  25.6 Biker toont de pagina ‘betaling niet gelukt’. |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |
|  | |  |

# Use case diagram

# Wireframes

# Maatregelen gegevensbescherming

## Uitgangspunten informatiebeveiliging “Biker”

### Het belang van informatie

Gegevens die verloren raken, ICT-systemen die uitvallen, of het lekken van klantgegevens naar onbevoegden en het veranderen van data kan ernstige gevolgen hebben voor het opereren van Biker, leiden tot imagoschade of in het ergste geval een berisping van de Autoriteit Persoonsgegevens. Dergelijke gevallen kunnen leiden tot negatieve consequenties voor ketenpartners, leveranciers, klanten en de organisatie Biker.

Deswege is informatiebeveiliging een belangrijk aspect voor het ontwerp van een functioneel systeem.

### Visie

Biker wil in het aankomende jaar een online platform voor de verkoop, verhuur en reservering van elektrische fietsen, damesfietsen, herenfietsen, bijbehorende accessoires en het aanbieden van reizen georganiseerde door externe partijen ontwikkelen.

Voor het goed functioneren van dit online platform van Biker is het zeer belangrijk dat er een betrouwbare informatievoorziening tot stand komt. Deze is noodzakelijk zowel voor het functioneren van Biker en als basis voor het beschermen van rechters van klanten en bedrijven, zoals vastgesteld in de Algemene Verordening Gegevensbescherming (AVG). Noodzakelijk hiervoor is bewustzijn omtrent de risico’s die gepaard gaan met de verwerking en opslag van deze gegevens.

### Doelstelling

Het beleid omtrent informatiebeveiliging, ookwel het IB-beleid genoemd, schept een kader voor het nemen van de juiste maatregelen op zowel technisch als organisatorisch vlak, om zo klant-gerelateerde en operationeel-kritische informatie te beschermen en de juistheid hiervan te garanderen. Tevens is dit van belang om ervoor te zorgen dat Biker zich houdt aan de relevante wetgeving. Biker streeft ernaar om de controle over de datastromen en verstrekte gegevens te hebben en hierover verantwoording af te kunnen leggen. Dit houdt in dat het management van Biker weet welke maatregelen er genomen worden en dat dit opgenomen is in het organisatiebeleid.

### Uitgangspunten

* De informatiebeveiliging van Biker voldoet aan de wetgeving in het algemeen en AVG in het bijzonder.
* Het IB-beleid wordt vastgesteld door het management van Biker. De directie bespreekt regelmatig het IB-beleid en voert waar nodig wijzigingen door.
* De beslissingen hierin worden gebaseerd op de Code voor Informatiebeveiliging (NEN/ISO 27002).

### Risicobenadering

Het informatiebeleid van Biker is gebaseerd op de te verwachten risico’s. Dit houdt in dat de maatregelen tot stand komen op basis van de ISO 27002 certificering.

De eigenaar van het system analyseert de kwetsbare onderdelen van het systeem door middel van een risicobeschrijving. Hierbij houdt hij rekening met de wettelijke eisen omtrent de verwerking van de betreffende gegevens. Hiervoor wordt de formule **risico = kans x impact** gehanteerd.

### Doelgroepen

Het IB-beleid van Biker is bedoeld voor alle in- en externe medewerkers van Biker:

|  |  |
| --- | --- |
| Doelgroep | Relevantie voor IB-beleid |
| Investeerders | Risicobescherming investering |
| Eigenaar | Risicobescherming wettelijke aansprakelijkheid |
| Directie | Kaderstelling en implementatie |
| Management | Sturing op informatieveiligheid en controle op naleving |
| Medewerkers | Gedrag en naleving |
| Facilitaire zaken | Fysieke toegangsbeveiliging |
| Personeelszaken | Arbeidsvoorwaardelijke zaken |
| ICT-diensten | Technische beveiliging |
| Auditors | Onafhankelijke toetsing |
| Leveranciers | Compliance |
| Ketenpartners | Compliance |

### Scope

De scope van dit beleid bestaat uit alle system, processen, verwerkingen, informatie en gegevens van zowel de werknemers, klanten en ketenpartners van Biker. Hierbij wordt uitgegaan van het gebruik van deze gegevens in de meest brede vorm, dus bestaande uit alle mogelijke locaties, systemen en tijdstippen van gebruik.

### IB-beleid en architectuur

Het informatiebeleid (IB-beleid) is onderdeel van het informatiebeleid van Biker. Hiertoe behoren onder andere richtlijnen, maatregelen en uitganspunten, welke uitgewerkt zijn in een classificering verscheidene beschermingsniveaus.

### Werking

Dit informatiebeleid heeft als ingangsdatum de eerste werkdag na goedkeuring van de directie en investeerders van Biker. Deze vervangt dan per direct het voorgaande informatiebeleid van Biker uit 2017.

## Organisatie van de informatiebeveiliging

### Interne organisatie

#### Risico’s

De belangrijkste risico’s omtrent de interne organisatie omvatten onder andere het niet expliciet toekennen van verantwoordelijkheden, het niet uitvoeren van de omschreven maatregelen, of het gebruik van systemen en apparaten welke volgens dit beleid niet zijn goedgekeurd. Deze risico’s kunnen als resultaat hebben dat de te nemen maatregelen niet correct worden uitgevoerd, met als gevolg datalekken, imagoschade of ondermijning van de bedrijfscontinuïteit.

#### Doelstelling

Doel van dit informatiebeveiligingskader is het beheren van de informatie en het op correcte wijze beveiligen van deze gegevens binnen de organisatie.

Hiertoe wordt een kader geschept om de implementatie en het beheer van deze gegevens op correcte wijze uit te voeren.

Tot slot is het doel van dit document de uiteindelijke goedkeuring van de te nemen maatregelen en implementaties van technische interventies door het management van Biker, teneinde een draagvlak te kunnen neerzetten onder de medewerkers van des genoemde organisatie.

#### Verantwoordelijkheden

* De directie is eindverantwoordelijke voor alle beslissingen omtrent te beveiliging van data en gegevens binnen de organisatie Biker.
  + De directie gaat akkoord met de in dit document overeengekomen doelstellingen en werkwijzen, teneinde te voldoen aan de geldende wetgeving en de ‘best practices’ in de branche waarbinnen geopereerd wordt.
* De directie is eindverantwoordelijke voor het leveren van sturing omtrent de beveiligingsmaatregelen.
  + Geeft advies over de te verwachten risico’s.
  + Controleert of de te nemen maatregelen passen bij de eisen die hieraan gesteld worden en of deze inderdaad afdoende bescherming opleveren.
  + Evalueert tenminste jaarlijks het informatiebeleid en voert wijzigingen door.
* De afdeling Human Resources is verantwoordelijk voor de uitvoering van de gekozen maatregelen.
* De ICT-afdeling.
  + Zorgt voor zorgvuldige loginstrumenten, het monitoren hiervan en voor correcte afhandeling van mogelijke incidenten.
  + Neemt technische maatregelen en levert hierin advies.
  + Is verantwoordelijk voor beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen, die voortvloeien uit betrouwbaarheidseisen.
  + Is verantwoordelijk voor alle beheeraspecten van informatiebeveiliging, zoals ICT Security Management.

### Taken en rollen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Wie | Plan:  Kaderstelling | Do:  Uitvoering | Check:  Controle | Act:  Verbetering |
| Sturen:  Directie  Dagelijkse uitvoering: CIO | Ontwikkelen van kaders (beleid en architectuur);  Reglementen. | Inbedding AVG;  Advisering;  Crisisbeheersing. | Controle;  Audit;  Penetratietesten. | Bijsturen: Opdrachtverstrekking voor verbeteracties;  Rapportage aan directie. |
| Vragen:  Alle afdelingen | Formuleren van beveiligingseisen en opstellen beleid en beveiligingsplannen | Stimuleren van beveiligings-bewustzijn bij medewerkers, risico- en bedrijfs-continuïteit-management. | Interne controle;  Sturen op naleving van regels door medewerkers;  Compliance. | Verbeteren bedrijfscontinuïteit;  Rapportage aan CIO. |
| Uitvoeren:  Service Organisatie (in uitvoerende rol) | Beleidsvoorbereiding.  Technische onderzoeken. | Leveren van security-management en services;  Incidentbeheer;  Logging;  Monitoring;  Advies. | Vulnerability scanning; evaluatie en rapportage. | Uitvoeren verbeteracties;  Advies aan de CIO over aanpassingen aan de informatievoorziening. |

### Functioneel overleg

De aangestelde functionaris gegevensbeveiliging stelt een team samen van medewerkers die verantwoordelijk zijn voor de informatiebeveiliging en heeft hier regelmatig een teamoverleg mee. Deze functionaris is tijdens dergelijke bijeenkomsten voorzitter. Het doel van het overleg is het leveren van advies, het opstellen van beleid en levert strategische of operationele maatregelen omtrent gegevensbeveiliging.

### Rapportage en escalatielijn voor IB

Medewerker 🡪 Chef 🡪 Security verantwoordelijke 🡪 Management 🡪 CIO 🡪 Directie 🡪 Eigenaar 🡪 College Bescherming Persoonsgegevens/ Autoriteit Persoonsgegevens.

#### Externe partijen

* Het informatiebeleid en relevante wetgeving geldt ook voor alle ketenpartners en/of leveranciers waar Biker mee samenwerkt of gegevensverkeer mee deelt.
* Bij een contract gelden altijd de Algemene Inkoop Voorwaarden (AIV).
* Ook voor leveranciers of overige derde partijen geldt het ‘comply or explain’ beginsel, welke inhoudt dat deze partijen zich dienen te houden aan de in dit document opgestelde beveiligingseisen en duidelijkheid moeten geven omtrent de redenatie achter het niet opvolgen van een specifieke bepaling.
* Voor gegevensverkeer, datakoppelingen of dataopslag met derden, is dit informatiebeveiligingsbeleid ook van toepassing. Het belangrijkste doel hierbij is risicobeheersing.
* De beveiligingsmaatregelen tussen Biker en ketenpartners en/of leveranciers worden specifiek vastgelegd in bewerkersovereenkomsten, in overeenstemming met de relevante bepalingen uit de Algemene Verordening Gegevensbescherming (AVG).

#### ICT Crisisbeheersing

Om tijdens een crisis adequaat te kunnen reageren, dient de functionaris gegevensbescherming en het management van de afdeling ICT een team samen te stellen van competente professionals om hier snel, adequaat en efficiënt op te kunnen reageren.

## Beheer van bedrijfsmiddelen

### Verantwoordelijkheid voor bedrijfsmiddelen

#### Risico’s

Belangrijkste risico’s omtrent bedrijfsmiddelen zijn diefstal, misbruik (al dan niet met opzet) en beschadiging of verouderde software. Tevens kan het mogelijk onduidelijk zijn wie eindverantwoordelijke is voor de gegevens of updates omtrent het systeem, waardoor deze beveiliging hier suboptimaal ingericht kan zijn.

Tot slot is onbevoegde toegang tot de systemen van Biker door derden, alsook onbevoegde gegevensinzage door externe partijen waar Biker mee samenwerkt, een risico welke zoveel mogelijk afgedekt dient te worden.

#### Beheersmaatregelen

* Het gebruik van gegevens, systemen en/of apparaten toebehorend aan Biker zijn niet toegestaan in de privésfeer.
* Een medewerker zorgt ervoor dat hij of zij zorgvuldig met bedrijfsinformatie en persoonsgegevens van Biker, ketenpartners en/of klanten omgaat. Hier wordt met name zorg gedragen tegen verlies en/of diefstal.
* Klantgegevens, en hiermee persoonsgegevens, worden door medewerkers uitsluiten gebruikt voor het uitvoeren van taken waarvoor deze gegevens bedoeld zijn. Verder dienen medewerkers alleen taken uit te voeren die passend zijn bij de rol waarbinnen ze op dat moment opereren.
* Alle systemen, apparaten en dergelijke moeten duidelijk gedocumenteerd zijn in een inventaris. Deze dient tenminste maandelijks geüpdatet te worden.
* Alle gegevens, systemen, apparaten hebben een specifiek genoemde verantwoordelijke, welke zorg draagt voor de juiste omgang met de gegevens en/of systemen en het voldoen aan de in dit document opgestelde eisen.

### Classificatie van informatie

Binnen het informatiebeveiligingsbeleid van Biker wordt gebruik gemaakt van classificatie van gevoeligheid van informatie, gegevens en systemen. Hierdoor wordt inzichtelijk welke maatregelen genomen dienen te worden voor een juiste omgang omtrent de beveiliging. Hierbij wordt rekening gehouden met de drie betrouwbaarheidsaspecten van gegevens: beschikbaarheid, vertrouwelijkheid en integriteit.

#### Risico’s

* Het ontbreken van classificatie, of het hebben van een onjuiste classificatie, kan ten gevolge hebben dat informatie onvoldoende beschermd wordt, met mogelijk een datalek ten gevolge.
* Tevens is het mogelijk dat bepaalde informatie te hoog is geclassificeerd, waardoor er onnodige maatregelen genomen worden, welke kosten met zich meebrengen.
* Zonder classificatie, of bij verkeerde inschaling, zal het onduidelijk zijn welke systemen en/of gegevens bedrijfskritische systemen en/of gegevens zijn. Hierdoor kan de bedrijfscontinuïteit van Biker in gevaar komen.

#### Doelstellingen

Doelstelling is dat gegevens en systemen een juist niveau van bescherming en beveiliging hebben.

Verder wordt in dit gedeelte de classificatie van gegevens uitgewerkt ten bate van de hierboven vermelde punten.

#### Beheersmaatregelen

Als maatregel worden de gegevens geclassificeerd aan de hand van de relevante wetgeving, de gevoeligheid van de gegevens en de mate van belangrijkheid van deze gegevens voor de bedrijfscontinuïteit van Biker. Tevens worden er maatregelen en procedures uiteengezet voor de classificatie van de gegevens.

|  |  |  |  |
| --- | --- | --- | --- |
| **Niveau** | **Vertrouwelijkheid** | **Integriteit** | **Beschikbaarheid** |
| Geen | **Openbaar**  Informatie mag door iedereen worden ingezien | **Niet zeker**  Informatie mag worden veranderd | **Niet nodig**  Gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn |
| Laag | **Bedrijfsvertrouwelijkheid**  Informatie is toegankelijk voor alle medewerkers van de organisatie | **Beschermd**  Het bedrijfsproces staat enkele (integriteits-) fouten toe | **Noodzakelijk**  Informatie mag incidenteel niet beschikbaar zijn |
| Midden | **Vertrouwelijk**  Informatie is alleen toegankelijk voor een beperkte groep gebruikers | **Hoog**  Het bedrijfsproces staat zeer weinig fouten toe | **Belangrijk**  Informatie moet vrijwel altijd beschikbaar zijn; continuïteit is belangrijk |
| Hoog | **Geheim**  Informatie is alleen toegankelijk voor direct geadresseerde(n) | **Absoluut**  Het bedrijfsproces staat geen fouten toe | **Essentieel**  Informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten |

#### Uitgangspunten

* De bovenstaande tabel heeft als scope alle data, informatie, gegevens, systemen, apparatuur en netwerkonderdelen.
* De gegevens kunnen variabel zijn in de mate van gevoeligheid of noodzakelijkheid voor de bedrijfscontinuïteit. Voor bepaalde typen gegevens zijn extra maatregelen noodzakelijk.
* De eindverantwoordelijke van de informatie deelt deze in onder de juiste classificering. Wanneer er aan specifieke wet- en regelgeving voldaan dient te worden, moet deze expliciet beschreven worden.
* Er wordt telkens zo laag mogelijk geclassificeerd, aangezien een hoger niveau leidt tot onnodige kosten en overhead.
* Een technische maatregel geniet voorkeur over een verandering van gedrag bij de medewerkers.
* Getracht wordt om te zorgen voor een balans tussen de kosten van de maatregelen en het te verwachten risico.
* Er wordt geclassificeerd op basis van informatie. De classificatie wordt opgesteld door het management en de CIO en worden tenminste eenmaal per jaar gecontroleerd op juistheid en volledigheid.

#### toelichting

Zoals hierboven kort benoemd, worden de maatregelen en procedures opgesteld aan de hand van de risicoclassificatie, waarbij wordt gekeken naar de technische, operationele en financiële haalbaarheid van de maatregelen. Over het algemeen is het beleid dat als een marginale extra investering leidt tot aanzienlijk betere beveiliging, deze maatregelen genomen dienen te worden, hierbij rekening houdend met passende maatregelen gebaseerd op de classificatie uit bovenstaande tabel.

## Beveiliging van personeel

### Risico’s

Wanneer nieuwe medewerkers worden aangenomen of externen worden ingehuurd, kan dit extra risico’s teweegbrengen. Dit onder meer door de verhoogde kans op menselijke fouten, welke significante invloed kunnen hebben op de integriteit, vertrouwelijkheid en beschikbaarheid van de gegevens en systemen en informatie(verwerking).

### Doelstelling

Doel van dit onderdeel van het beveiligingsdocument is zorgen dat zowel de werknemers als externen duidelijkheid hebben over de werkwijze, risico’s en verantwoordelijkheden teneinde het risico van diefstal, foutief gebruik of fraude te reduceren.

De verantwoordelijkheden ten aanzien van beveiliging is voor het dienstverband vastgelegd in passende functiebeschrijvingen en in de arbeidsvoorwaarden.

Zowel werknemers als externen en (keten)partners welke toegang hebben tot ICT-systemen of bedrijfs- en/of klantgegevens van Biker, zullen een overeenkomsten tekenen over de informatiebeveiligingsmaatregelen en -rollen met bijbehorende verantwoordelijkheden.

### Beheersmaatregelen

* Medewerkers die in aanraking komen met persoonsgegevens zullen een Verklaring Omtrent het Gedrag (VOG) aanleveren voor de ingang van de eerste werkdag.
* De manager is eindverantwoordelijke voor het inrichten van de beveiliging, het wijzigen of beëindigen van een dienstverband of een overeenkomst met derden. Dit alles gebeurd onder toezicht van de HR-afdeling.
* Wanneer een dienstverband wordt ontbonden, dienen alle apparatuur, toegangscodes en overige informatie omtrent Biker te worden ingeleverd. De autorisaties omtrent de systemen van Biker worden ingetrokken en geblokkeerd.
* Medewerkers dienen voor volledige indiensttreding een training te krijgen omtrent de maatregelen en procedures die volgen uit het informatiebeleid van Biker.

### Bewustwording

* Het management draagt zorg dat alle medewerkers voldoen aan de in dit document opgestelde beveiligingsrichtlijnen.
* De directie draagt zorg voor de communicatie op organisatieniveau en de bewustwording en scholing omtrent informatieveiligheid.
* De directie bevordert algehele communicatie en bewustwording rondom informatieveiligheid.
* In werkoverleggen wordt regelmatig de informatiebeveiliging besproken.

## Fysieke beveiliging en beveiliging van de omgeving

### Risico’s

Tot de risico’s behoren het onrechtmatig verkrijgen van toegang tot systemen en/of (persoons)gegevens door medewerkers en/of derden. Wanneer hieromtrent geen afdoende registratie plaatsvindt zijn dergelijke incidenten bovendien niet tot een specifiek persoon te herleiden.

Door het feit dat de medewerkers op meerdere locaties ingeplant kunnen worden, alsook het openstellen van de panden voor klanten, welke tevens in reparatie- en verkoopgedeelten kunnen komen, is het eenvoudig voor niet-medewerkers om toegang tot panden en systemen te krijgen. Hier dienen afdoende maatregelen tegen genomen te worden.

## Beveiliging van apparatuur en informatie

#### Risico’s

* Foutieve autorisaties kunnen ten gevolge hebben dat er onjuiste handeling of misbruik plaatsvindt.
* Het onvolledig, onjuist documenteren alsook het ontbreken van documentatie kan ten gevolge hebben dat gegevens op een foutieve wijze worden verwerkt, of tot problemen rondom de bedrijfscontinuïteit leiden.
* Het niet uitvoeren en vastleggen van technische en functionele tests en/of de resultaten hiervan, kan leiden tot een verhoogd risico van uitval en/of gegevensverlies.
* Systemen en netwerken zijn gevoelig voor trojans, virussen en hackpogingen.

#### doelstelling

* Doelstelling van dit onderdeel van het informatiebeveiligingsplan is zorgt dragen voor correct gebruik van de ICT-systemen en netwerken.
* Tevens dienen de maatregelen, procedures en verantwoordelijkheden voor het inrichten en onderhouden alsook het gebruik van ICT-systemen en apparatuur teneinde de hiermee gepaarde risico’s zoveel mogelijk te mitigeren.

### Beheersmaatregelen

#### Organisatorische aspecten

* Autorisaties en toegang tot verscheidene onderdelen van de systemen van Biker dienen zoveel mogelijk uitgesplitst te worden. In principe zou geen enkele medewerker autorisaties mogen hebben die ervoor kunnen zorgen dat beschikbaarheid, integriteit en/of vertrouwelijkheid in het geding kunnen raken.
* Indien bovenstaande toch noodzakelijk blijkt te zijn, zal er logging plaatsvinden over de activiteiten van deze gebruiker om eventuele wijzigingen te kunnen herstellen.
* Er is een scheiding tussen beheertaken en overige gebruikstaken. Alleen wanneer er als beheerder is ingelogd, kunnen dergelijke werkzaamheden plaatsvinden.
* Bij externe hosting van gegevens, informatie en/of processen blijft Biker eindverantwoordelijk voor de betrouwbaarheid van de geleverde diensten richting klant en/of ketenpartners.

#### technische aspecten

* Op de diverse onderdelen van de informatiestructuren binnen Biker (apparatuur, netwerken e.d.) worden firewalls en/of antivirussoftware van diverse leveranciers geïnstalleerd.
* Documenten zoals brieven en/of facturen worden op een correcte wijze opgeslagen en er wordt bijgehouden welke werknemer op welk moment toegang heeft gehad tot het archief.
* Alle data welke geclassificeerd is volgens een classificatieniveau hoger dan ‘geen’ worden geencrypt, teneinde hiermee te voldoen aan de bepalingen omtrent de Algemene Verordening Gegevensbescherming (AVG).
* Bij dergelijke classificaties wordt gehouden aan de bepalingen omtrent de relevante beveiligingseisen zoals elders in dit document vastgesteld.

#### back-up en recovery

Alle bestanden, gevoelige en/of kritische informatie, dienen regelmatig geback-upt te worden, teneinde de bedrijfscontinuïteit te garanderen.

#### informatie-uitwisseling

Er worden geen persoonsinformatie en/of klantgegevens met derden gedeeld, tenzij absoluut noodzakelijk of om te voldoen aan geldende wet- en regelgeving. Bij dergelijke situaties wordt alleen de absoluut noodzakelijke informatie gedeeld.

#### Controle

* Het gebruik van informatiesystemen, alsmede uitzonderingen en informatiebeveiligingsincidenten, worden vastgelegd in logbestanden op een dergelijke manier dat tenminste wordt voldaan aan alle relevante wettelijke eisen. Relevante data om te loggen zijn:
  + Type gebeurtenis
  + Handelingen met speciale bevoegdheden
  + Systeemwaarschuwingen
  + Ongeautoriseerde toegang
  + Wijzigingen van instellingen
* Een logregel bevat minimaal:
  + Een gebruikersnaam of ID
  + De gebeurtenis
  + De ID van het werkstation
  + Het resultaat van de handeling
  + Datum en tijdstip van de gebeurtenis
* In een logregel worden alleen de voor de rapportage noodzakelijke gegevens opgeslagen

### Beheer van de dienstverlening door een derde partij

#### risico’s

Bij beheer van systemen en gegevens door een derde partij kan ook informatie van Biker op straat komen te liggen. Biker blijft verantwoordelijk voor de beveiliging van zijn gegevens in dit deel van de keten.

#### doelstelling

Doel is om te zorgen dat de informatiebeveiliging passend is bij de te verwachten risico’s en calamiteiten. Deze dienen in relatie tot derden vastgelegd te worden in bewerkersovereenkomsten, teneinde te voldoen aan de bepalingen uit de Algemene Verordening Gegevensbescherming (AVG).

#### beheersmaatregelen

De te nemen maatregelen omtrent de beveiliging zullen in iedere overeenkomst of contractuele verplichting uitdrukkelijk omschreven worden. Mocht dit niet het geval zijn, dan zijn de bepalingen en maatregelen uit dit document leidend. Tevens zal Biker regelmatig audits bij de (keten)partners en gegevensverwerkers laten uitvoeren.

### Behandeling van media

#### risico’s

Bij vluchtige media (bijvoorbeeld USB en verwijderbaar geheugen alsook papieren) kan de hierop aanwezige informatie in verkeerde handen vallen. Dit met name omtrent zaken als verlies en/of diefstal.

#### doelstelling

Doelstelling is het voorkomen van datalekken omtrent persoonsgegevens en/of bedrijfsgevoelige informatie.

#### beheersmaatregelen

* Er dienen procedures te worden vastgesteld voor het beheer van verwijderbare media
* Er dienen procedures te worden vastgesteld voor het op een veilige manier verwijderen van media als ze niet langer nodig zijn.
* Systeemdocumentatie dient te worden beschermd tegen onbevoegde toegang.

#### uitgangspunten

* Er zijn procedures voor het beheer van verwijderbare media en voor het veilig verwijderen of hergebruiken van ICT-apparatuur
* Harde schijven en andere media worden adequaat gewist of vernietigd bij afstoting of hergebruik.
* Er zijn richtlijnen voor het opbergen van papieren en computermedia.
* Innamebeleid voor mobiele apparatuur, wanneer deze niet meer worden gebruikt.

### Uitwisseling van informatie

#### risico’s

Verlies of diefstal van laptops, usb-sticks e.d. waarbij bovendien informatie in verkeerde handen komt. Tevens is het mogelijk dat de ontvanger van de informatie deze gebruikt voor doeleinden welke niet passen bij de opgegeven doelen ten tijde van levering van desbetreffende informatie.

#### beheersmaatregelen

* Er dient een integraal beleid te worden opgesteld inclusief de te nemen maatregelen en de procedures om te uitwisseling van informatie te beschermen.
* Teneinde bovengenoemd doel zullen er overeenkomsten gesloten worden, waarin de relevante aspecten duidelijk overeengekomen zullen worden.
* Bij uitwisseling van informatie omtrent persoonsgegevens en/of bedrijfskritische informatie dient deze op een passend niveau beschermd te worden.

## Logische toegangsbeveiliging

### Authenticatie en autorisatie

* Wachtwoorden worden voor een beperkte periode toegekend (3 tot maximaal 6 maanden).
* Wachtwoorden dienen aan eisen te voldoen, deze worden afgedwongen door het systeem.
* De gebruiker is verantwoordelijk voor het geheim blijven van zijn wachtwoord.
* Authenticatiemiddelen zoals wachtwoorden worden beschermd tegen inzage en wijziging door onbevoegden tijdens transport en opslag (door middel van encryptie).
* Autorisatie is rol gebaseerd. Autorisaties worden toegekend via functie(s) en organisatieonderdelen.

### Mobiel en thuiswerken

Er is bij Biker geen mogelijkheid tot thuiswerken. Verder mag er geen klantinformatie gedeeld worden op private apparatuur. Alle communicatie verloopt via de apparatuur en systemen van Biker.

De netwerken en systemen van Biker worden waar mogelijk gescheiden, zodat een fout in een van de systemen niet een organisatie brede uitval ten gevolge heeft.

### Beveiliging van informatiesystemen (software).

#### softwareontwikkeling en onderhoud

* Applicaties worden ontwikkeld en getest o.b.v. de code voor informatiebeveiliging. Er wordt tenminste getest op bekende kwetsbaarheden.
* Webapplicaties worden voor de in productie name onder meer getest op invoer van gegevens (grenswaarden, format, inconsistentie, SQL-injectie, cross site scripting, etc.).
* De uitvoerfuncties van programma’s maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen (bijv. door checksums).
* Alleen gegevens die noodzakelijk zijn voor de gebruiker worden uitgevoerd (doelbinding), rekening houdend met beveiligingseisen (classificatie).
* Toegang tot de broncode is beperkt tot de medewerkers, die deze code onderhouden of installeren.
* Technische kwetsbaarheden worden regulier met een minimum van 4 keer per jaar gerepareerd door ‘patchen’ van software, of ‘ad hoc’ bij acute dreiging.

#### encryptie

Alle persoonsgegevens dienen encrypted te worden opgeslagen, teneinde de risico’s omtrent lekken of ontvreemding van deze data te minimaliseren.

## Beveiligingsincidenten

### Melding en registratie

* Bij het vermoeden of constateren van een beveiligingslek onderneemt de medewerker de in dit document omschreven stappen. Deze bestaan tenminste uit het direct melden van dit beveiligingslek bij de functionaris informatiebeveiliging van Biker.
* De door een medewerker geconstateerde of kenbaar gemaakte beveiligingsincidenten dienen te worden geregistreerd. Deze registratie dient te worden overlegd aan de functionaris informatiebeveiliging van Biker.
* Wanneer het beveiligingsincident een datalek omtrent persoonsgegevens betreft, dient er een melding te worden gemaakt bij het College Bescherming Persoonsgegevens, zoals vastgesteld in de Algemene Verordening Gegevensbescherming (AVG).

## Bedrijfscontinuïteit

### Risico’s

Wanneer er geen planning bestaat betreffende de continuïteit van de systemen en gegevens van Biker, zal dit in het ergste geval kunnen leiden tot de uitval van het bedrijfsmatig opereren van Biker.

### Doelstelling

Onderbreken van bedrijfsactiviteiten tegengaan en kritische bedrijfsprocessen beschermen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstellingen.

Een adequaat beheerproces van bedrijfscontinuïteit om de uitwerking op de organisatie, veroorzaakt door het verlies van informatie en het herstellen daarvan tot een aanvaardbaar niveau te beperken.

Informatiebeveiliging is een integraal onderdeel van het totale bedrijfscontinuïteitsproces en andere beheerprocessen binnen de organisatie.

## Naleving

### (Wettelijke) kaders

De informatie welke wordt verwerkt door Biker betreft voornamelijk klantinformatie. Hieronder valt ook een gedeelte persoonsgegevens. De relevante wetgeving voor omgang met dit type informatie is vastgelegd in de Algemene Verordening Gegevensbescherming (AVG). Hieronder volgen een aantal relevante bepalingen uit de AVG waar tijdens zowel de ontwerp- als beheerfase rekening mee gehouden dient te worden.

Deze onderstaande bepalingen en hoe deze eisen worden ingepast in het dagelijks opereren van Biker zijn (gedeeltelijk) verwerkt in bovenstaand beveiligingsplan. Overige, niet ingepaste informatie, is relevant voor een technisch ontwerp en zal in dit stadium worden toegevoegd aan de documentatie.

# Bijlage 1: Relevante bepalingen avg

Bepaling 26

* Gepseudonimiseerde persoonsgegevens die door het gebruik van aanvullende gegevens aan natuurlijke persoon kunnen worden gekoppeld, moeten als gegevens over een identificeerbare natuurlijke persoon worden beschouwd.
* Om te bepalen of een natuurlijke persoon identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken.
* Om uit te maken of van middelen redelijkerwijs valt te verwachten dat zij zullen worden gebruikt om de natuurlijke persoon te identificeren, moet rekening worden gehouden met alle objectieve factoren, zoals de kosten van en de tijd benodigd voor identificatie, met inachtneming van de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen.
* De gegevensbeschermingsbeginselen dienen derhalve niet van toepassing te zijn op anonieme gegevens, namelijk gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is.
* Deze verordening heeft derhalve geen betrekking op de verwerking van dergelijke anonieme gegevens, onder meer voor statistische of onderzoeksdoeleinden.

Bepaling 27

* De onderhavige verordening is niet van toepassing op de persoonsgegevens van overleden personen

Bepaling 28

* De toepassing van pseudonimisering op persoonsgegevens kan de risico’s voor de betrokkenen verminderen en de verwerkingsverantwoordelijken en de verwerkers helpen om hun verplichtingen inzake gegevensbescherming na te komen. De uitdrukkelijke invoeren van “pseudonimisering” in deze verordening is niet bedoeld om andere gegevensbeschermingsmaatregelen uit te sluiten.

Bepaling 29

* Om stimuli te creëren voor pseudonimisering bij de verwerking van persoonsgegevens zouden, terwijl een algemene analyse mogelijk blijft, pseudonimiseringsmaatregelen moeten kunnen worden genomen door dezelfde verwerkingsverantwoordelijke wanneer deze de noodzakelijke technische en organisatorische maatregelen heeft getroffen om er bij de desbetreffende verwerking voor te zorgen dat deze verordening ten uitvoer wordt gelegd, en dat de aanvullende gegevens om de persoonsgegevens aan een specifieke betrokkene te koppelen, apart worden bewaard. De verwerkingsverantwoordelijke die de persoonsgegevens verwerkt, moet aangeven wie bij dezelfde verwerkingsverantwoordelijke gemachtigde personen zijn.

Bepaling 30

* Natuurlijke personen kunnen worden gekoppeld aan online-identificatoren via hun apparatuur, applicaties, instrumenten en protocollen, zoals IP-adressen, identificatiecookies of andere identificatoren zoals radiofrequentie-identificatietags. Dit kan sporen achterlaten die, met name wanneer zij met unieke identificatoren en andere door de servers ontvangen informatie worden gecombineerd, kunnen worden gebruikt om profielen op te stellen van natuurlijke personen en natuurlijke personen te herkennen

Bepaling 32

* Toestemming dient te worden gegeven door middel van een duidelijke actieve handeling, bijvoorbeeld een schriftelijke verklaring, ook met elektronische middelen, of een mondelinge verklaring, waaruit blijkt dat de betrokkene vrijelijk, specifiek, geïnformeerd en ondubbelzinnig met de verwerking van zijn persoonsgegevens instemt.
* Hiertoe zou kunnen behoren het klikken op een vakje bij een bezoek aan een internetwebsite, het selecteren van technische instellingen voor diensten van de informatiemaatschappij of een andere verklaring of een andere handeling waaruit in dit verband duidelijk blijkt dat de betrokkene instemt met de voorgestelde verwerking van zijn persoonsgegevens.
* Stilzwijgen, het gebruik van reeds aangekruiste vakjes of inactiviteit mag derhalve niet als toestemming gelden.
* De toestemming moet gelden voor alle verwerkingsactiviteiten die hetzelfde doel of dezelfde doeleinden dienen.
* Indien de verwerking meerdere doeleinden heeft, moet toestemming voor elk daarvan worden verleend.

Bepaling 36

* De hoofdvestiging van een verwerkingsverantwoordelijke in de Unie dient de plaats te zijn waar zich zijn centrale administratie in de Unie bevindt, tenzij de besluiten over de doeleinden van en de middelen voor de verwerking van persoonsgegevens worden genomen in een nadere vestiging van de verwerkingsverantwoordelijke in de Unie, in welk geval deze andere vestiging als hoofdvestiging moet worden beschouwd.
* Welke vestiging de hoofdvestiging van een verwerkingsverantwoordelijke in de Unie is, dient te worden bepaald op grond van objectieve criteria, zoals het effectief en daadwerkelijk uitvoeren van beheersactiviteiten, met het oog op het nemen van de kernbesluiten over de doelstellingen van en de middelen voor de verwerking via bestendige verhoudingen.

Bepaling 39

* Elke verwerking van persoonsgegevens dient behoorlijk en rechtmatig te geschieden. Voor natuurlijke personen dient het transparant te zijn dat hen betreffende persoonsgegevens worden verzameld, gebruikt, geraadpleegd of anderszins verwerkt en in hoeverre de persoonsgegevens worden verwerkt of zullen worden verwerkt.
* Overeenkomstig het transparantiebeginsel moeten informatie en communicatie in verband met de verwerking van die persoonsgegevens eenvoudig toegankelijk en begrijpelijk zijn, en moet duidelijke en eenvoudige taal worden gebruikt.
* De persoonsgegevens dienen toereikend en ter zake dienend te zijn en beperkt te blijven tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Dit vereist met name dat ervoor wordt gezorgd dat de opslagperiode van de persoonsgegevens tot een strikt minimum wordt beperkt.
* Persoonsgegevens mogen alleen worden verwerkt indien het doel van de verwerking niet redelijkerwijs op een andere wijze kan worden verwezenlijkt.
* Om ervoor te zorgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is, dient de verwerkingsverantwoordelijke termijnen vast te stellen voor het wissen van gegevens of voor een periodieke toetsing ervan.
* Alle redelijke maatregelen moeten worden genomen om ervoor te zorgen dat onjuiste persoonsgegevens worden gerectificeerd of gewist.
* Persoonsgegevens moeten worden verwerkt op een manier die een passende beveiliging en vertrouwelijkheid van die gegevens waarborgt, ook ter voorkoming van ongeoorloofde toegang tot of het ongeoorloofde gebruik van persoonsgegevens en de apparatuur die voor de verwerking wordt gebruikt.

Bepaling 40

* Voor rechtmatige verwerking van persoonsgegevens is de toestemming van de betrokkene vereist of een andere gerechtvaardigde grondslag waarin de wet voorziet, hetzij in deze verordening, hetzij in andere Unierechtelijke of lidstaatrechtelijke bepalingen als bedoeld in deze verordening, of ook dat de verwerking noodzakelijk is om te voldoen aan wettelijke verplichting die op de verwerkingsverantwoordelijke rust of om een overeenkomst uit te voeren waarbij de betrokkene partij is of om op verzoek van de betrokkene voorafgaand aan het aangaan van een overeenkomst maatregelen te nemen.

Bepaling 42

* Indien de verwerking plaatsvindt op grond van toestemming van de betrokkene, moet de verwerkingsverantwoordelijke kunnen aantonen dat de betrokkene toestemming heeft gegeven voor de verwerking.
* Met name in de context van een schriftelijke verklaring over een andere zaak dient te worden gewaarborgd dat de betrokkene zich ervan bewust is dat hij toestemming geeft en hoever deze toestemming reikt.

Bepaling 43

* Om ervoor te zorgen dat toestemming vrijelijk wordt verleend, mag toestemming geen geldige rechtsgrond zijn voor de verwerking van persoonsgegevens in een specifiek geval wanneer er sprake is van een duidelijke wanverhouding tussen de betrokkene en de verwerkingsverantwoordelijke, met name wanneer de verwerkingsverantwoordelijke een overheidsinstantie is, en dit het onwaarschijnlijk maakt dat de toestemming in alle omstandigheden van die specifieke situatie vrijelijk is verleend.
* De toestemming wordt geacht niet vrijelijk te zijn verleend indien geen afzonderlijke toestemming kan worden gegeven voor verschillende persoonsgegevensverwerkingen ondanks het feit dat dit in het individuele geval passend is, of indien de uitvoering van een overeenkomst, daaronder begrepen het verlenen van een dienst, afhankelijk is van de toestemming ondanks het feit dat dergelijke toestemming niet noodzakelijk is voor die uitvoering.

Bepaling 48

* Verwerkingsverantwoordelijken die deel uitmaken van een concern of een groep van instellingen die aan een centraal lichaam verbonden zijn, kunnen een gerechtvaardigd belang hebben bij de doorzending van persoonsgegevens binnen het concern voor interne administratieve doeleinden, waaronder de verwerking van persoonsgegevens van klanten of werknemers. De algemene beginselen voor de doorgifte van persoonsgegevens, binnen een concern, aan een in een derde land gevestigde onderneming blijven onverlet.

Bepaling 49

* De verwerking van persoonsgegevens voor zover die strikt noodzakelijk en evenredig is met het oog op netwerk- en informatiebeveiliging, d.w.z. dat een netwerk of informatiesysteem op een bepaald vertrouwelijkheidsniveau bestand is tegen incidentele gebeurtenissen of onrechtmatige of kwaadaardige acties die de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van opgeslagen of doorgegeven persoonsgegevens in het gedrang brengen, en de beveiliging van de daarmee verband houdende diensten die door deze netwerken en systemen worden geboden of via deze toegankelijk zijn, door overheidsinstanties, computercrisisteams (computer emergency response teams), computercalamiteitenteams (computer security incident response teams), aanbieders van elektronische communicatienetwerken en -diensten en aanbieders van beveiligingstechnologie en -diensten, vormt een gerechtvaardigd belang van de verwerkingsverantwoordelijke in kwestie. Zo kan er bijvoorbeeld sprake zijn van het verhinderen van ongeoorloofde toegang tot elektronische-communicatienetwerken en van verspreiding van kwaadaardige codes, alsook van het stoppen van “denial of service” – aanvallen en van schade aan computers en elektronische communicatiesystemen.

Bepaling 58

* Overeenkomstig het transparantiebeginsel moet informatie die bestemd is voor het publiek of voor de betrokkene beknopt, eenvoudig toegankelijk en begrijpelijk zijn en moet duidelijke en eenvoudige taal en, in voorkomend geval, aanvullend visualisatie worden gebruikt.
* Die informatie kan elektronisch worden verstrekt, bijvoorbeeld wanneer die tot het publiek is gericht, via een website.

Bepaling 59

* Er dienen regelingen voorhanden te zijn om de betrokkene in staat te stellen zijn rechten uit hoofde van deze verordening gemakkelijker uit te oefenen, zoals mechanismen om te verzoeken om met name inzage in en rectificatie of wissing van persoonsgegevens en, indien van toepassing, deze gratis te verkrijgen, alsmede om het recht van bezwaar uit te oefenen. De verwerkingsverantwoordelijke dient ook middelen te verstrekken om verzoeken elektronisch in te dienen, vooral wanneer persoonsgegevens langs elektronische weg worden verwerkt.
* De verwerkingsverantwoordelijke dient te worden verplicht onverwijld en ten laatste binnen een maand op een verzoek van de betrokkene te reageren, en om de redenen op te geven voor een eventuele voorgenomen weigering om aan dergelijke verzoeken gehoor te geven.

Bepaling 60

* Overeenkomstig de beginselen van behoorlijke en transparante verwerking moet de betrokkene op de hoogte worden gesteld van het feit dat er verwerking plaatsvindt en van de doeleinden daarvan.
* De verwerkingsverantwoordelijke dient de betrokkene de nadere informatie te verstrekken die noodzakelijk is om tegenover de betrokkene een behoorlijke en transparante verwerking te waarborgen, met inachtneming van de specifieke omstandigheden en de context waarin de persoonsgegevens worden verwerkt.
* Voorts moet de betrokkene worden geïnformeerd over het bestaan van profilering en de gevolgen daarvan.
* Indien de persoonsgegevens van de betrokkene moeten worden verkregen, moet hem worden meegedeeld of hij verplicht is de persoonsgegevens te verstrekken en wat de gevolgen zijn van niet-verstrekking van de gegevens.
* Die informatie kan met behulp van gestandaardiseerde icoontjes worden verstrekt, teneinde op goed zichtbare, begrijpelijke en duidelijk leesbare wijze de zin van de voorgenomen verwerking weer te geven.
* Elektronisch weergegeven icoontjes moeten machineleesbaar zijn.

Bepaling 63

* Een betrokkene moet het recht hebben om de persoonsgegevens die over hem zijn verzameld, in te zien, en om dat recht eenvoudig en met redelijke tussenpozen uit te oefenen, zodat hij zich van de verwerking op de hoogte kan stellen en de rechtmatigheid daarvan kan controleren.

Bepaling 64

* De verwerkingsverantwoordelijke dient, met name met betrekking tot onlinediensten en online-identificatoren, alle redelijke maatregelen te nemen om de identiteit te controleren van een betrokkene die om inzage verzoekt.
* Een verwerkingsverantwoordelijke mag persoonsgegevens niet uitsluitend bewaren om op eventuele verzoeken te kunnen reageren.

Bepaling 65

* Een betrokkene moet het recht hebben om hem betreffende persoonsgegevens te laten rectificeren en dient te beschikken over een “recht op vergetelheid” wanneer de bewaring van dergelijke gegevens inbreuk maakt op deze verordening (…)

Bepaling 66

* Ter versterking van het recht op vergetelheid in de onlineomgeving, dient het recht op wissing te worden uitgebreid door de verwerkingsverantwoordelijke die persoonsgegevens openbaar heeft gemaakt te verplichten de verwerkingsverantwoordelijken die deze persoonsgegevens verwerken, ervan op de hoogte te stellen dat de betrokkene heeft verzocht om het wissen van links naar, of kopieën of reproducties van die persoonsgegevens.
* Die verwerkingsverantwoordelijke dient daarbij, met inachtneming van de beschikbare technologie en de middelen waarover hij beschikt, redelijke maatregelen te nemen, waaronder technische maatregelen, om de verwerkingsverantwoordelijkheden die de persoonsgegevens verwerken, over het verzoek van de betrokkene te informeren.

Bepaling 67

* Tot de methoden ter beperking van de verwerking van persoonsgegevens zou kunnen behoren dat de geselecteerde persoonsgegevens tijdelijk naar een ander verwerkingssysteem worden overgebracht, dat de geselecteerde gegevens voor gebruikers niet beschikbaar worden gemaakt of dat gepubliceerde gegevens tijdelijk van een website worden gehaald.
* In geautomatiseerde bestanden moet in beginsel met technische middelen worden gezorgd voor een zodanige beperking van de verwerking van persoonsgegevens dat de persoonsgegevens niet verder kunnen worden verwerkt en niet kunnen worden gewijzigd.
* Het feit dat de verwerking van persoonsgegevens beperkt is, moet duidelijk in het bestand zijn aangegeven.

Bepaling 68

* Om de zeggenschap over zijn eigen gegevens verder te versterken, dient de betrokkene wanneer de persoonsgegevens via geautomatiseerde procedés worden verwerkt, ook de mogelijkheid te hebben de hem betreffende persoonsgegevens die hij aan een verwerkingsverantwoordelijke heeft verstrekt, in een gestructureerd, gangbaar, machineleesbaar en interoperabel formaat te verkrijgen en die aan een andere verwerkingsverantwoordelijke door te zenden.

Bepaling 70

* Wanneer persoonsgegevens worden verwerkt ten behoeve van direct marketing dient de betrokkene, ongeacht of het een aanvankelijke dan wel een verdere verwerking betreft, het recht te hebben te allen tijde en kosteloos bezwaar te maken tegen deze verwerking, ook in het geval van profilering voor zover deze betrekking heeft op de direct marketing.
* Dat recht moet uitdrukkelijk, op duidelijke wijze en gescheiden van overige informatie, onder de aandacht van de betrokkene worden gebracht.

Bepaling 71

* De betrokkene dient het recht te hebben niet te worden onderworpen aan een louter op geautomatiseerde verwerking gebaseerd besluit, dat een maatregel kan behelzen – over persoonlijke hem betreffende aspecten, waaraan voor hem rechtsgevolgen zijn verbonden of dat hem op vergelijkbare wijze aanmerkelijk treft, zoals de automatische weigering van een online ingediende kredietaanvraag of van verwerking van sollicitaties via internet zonder menselijke tussenkomst.
* Een verwerking van die aard omvat “profilering”, wat bestaat in de geautomatiseerde verwerking van persoonsgegevens ter beoordeling van persoonlijke aspecten van een natuurlijke persoon, (…)