DPIA | Model op basis van het rijksmodel

Betrokken bij het opstellen DPIA

EasySecure International B.V.	Booking Experts	
Vakantiepark de Witte Berg	Restaurant Bie Heintje	

Telefonisch	+31 (0541) 291 605
E-mail	info@dewitteberg.nl
	Vakantiepark de Witte Berg
Post	Wittebergweg 9
	7637 PM Oud Ootmarsum

Inhoudsopgave

Inleiding

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (hierna: AVG) in werking getreden. In de AVG is het verplicht om een Data Protection Impact Assessment (hierna: DPIA) uit te voeren als er een nieuwe of te wijzigen verwerking van persoonsgegevens kan leiden tot een mogelijk hoog risico voor de rechten en vrijheden van natuurlijke personen, ook wel de rechten van betrokkenen genoemd.

Met dit model kan een zoals bedoeld in de AVG worden uitgevoerd. Dit model is gebaseerd op *Model gegevensbeschermingseffectbeoordeling Rijksdienst (PIA)*. Met deze DPIA kunnen op structurele wijze mogelijke risico's met betrekking tot de rechten van natuurlijke personen (betrokkenen) in kaart gebracht. Vervolgens kunnen in deze DPIA maatregelen worden geselecteerd om de mogelijke risico's te mitigeren of te compenseren.

De DPIA bestaat uit 5 onderdelen:

A. Kenmerken

Hier worden op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen beschreven. Hierbij worden ook de middelen – waaronder in ieder geval gebruikte technologieën en eventuele verwerkers – beschreven die de verwerking van persoonsgegevens mogelijk maken.

B. Beoordeling rechtmatigheid

Hier wordt de rechtsgrond, noodzaak en doelbinding van de voorgenomen gegevensverwerkingen en rechten van de betrokkene beoordeeld.

C. Risico's

Hier worden de risico's van de voorgenomen gegevensverwerkingen voor de rechten van betrokkenen beschreven en beoordeeld. Hierbij wordt rekening gehouden met de aard, omvang, context en doelen van de voorgenomen gegevensverwerkingen. Met andere woorden, welke risico's zijn er bij deze verwerkingen.

D. Maatregelen

Dit gaat om de mogelijke maatregelen om de geïdentificeerde risico's van de voorgenomen gegevensverwerkingen voor de rechten van betrokkenen te adresseren ofwel de risico's te vermijden of kleiner te maken.

E. Doorlopende controle

Hier kunnen wijzigingen met betrekking tot de DPIA worden bijgehouden. Daarmee kunnen wijzigingen in de verwerkingen en de mogelijke risico's voor de rechten van natuurlijke personen (betrokkenen) in kaart gebracht worden.

A. Beschrijving kenmerken

Hieronder kan f op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

1. Voorstel

Beschrijf het voorstel waar de PIA op ziet en de context waarbinnen deze plaatsvindt op hoofdlijnen.

In Nederland geldt sinds mei 2018 de AVG en de UAVG en niet meer de Wbp. Op grond daarvan zijn de maatregelen ten aanzien van de bescherming persoonsgegevens opnieuw beoordeeld en herzien. Dat heeft geleid tot deze DPIA.

Systemen: IdentySoft
Dit systeem wordt gebruikt voor toegangscontrole tot het zwembad. Gegevens worden vastgelegd in dit systeem en voor deze doelen ook gebruikt.

Met IdentySoft kan invulling gegeven worden aan de hiervoor kort omschreven doelen.

Achtergrond van deze DPIA
Het voorliggende MODEL Data Protection Impact Assessment (hierna: DPIA) beoordeelt de
- privacyaspecten,
- de privacyrisico's bij het registreren, wijzigen en raadplegen van de toegangsregistratie
- Het registeren, wijzigen en raadplegen van deze gegevens zijn processen die gebruikmaken van IdentySoft, dat invulling geeft aan de hiervoor omschreven doelen.

In scope van deze DPIA:
- Het gaat om aanmaken van een account, aanmaken toegangspassen, kaarten, codes, toegangsrechten.

2. Persoonsgegevens

Som **alle categorieën van persoonsgegevens** op die worden verwerkt. Geef per categorie van betrokkene aan welke persoonsgegevens van hen verwerkt worden. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk, gevoelig en wettelijk identificatienummer.

A. Naam tabel met gegevens

Naam tabel: Users

Attribuut	Omschrijving	Type	Verplicht	Bron
User-ID	Intern nummer	gewoon	verplicht	automatisch door systeem
Voornaam	Voornaam medewerker	gewoon	verplicht [1]	administrator

[1] Er kan elk willekeurig teken ingevuld worden, dit geldt voor voor- en achternaam

Achternaam	Achternaam medewerker incl. tussenvoegsels	gewoon	verplicht	administrator
Startdatum	Startdatum toegang	gewoon	verplicht [2]	administrator
Einddatum	Einddatum toegang	gewoon	verplicht	automatisch door systeem
Toegangsgroep	Vastgelegde toegangstidstippen/toegangsregels	gewoon	nee	administrator
Tekstvelden	Vrij in te vullen, die niet voor het proces worden gebruikt	gewoon	nee	administrator
Card-ID	Gecodeerd card	gewoon	nee	administrator
Toegangscode	Toegangscode	gewoon	nee	administrator

Naam tabel: Templates

Attribuut	Omschrijving	type	Verplicht	Bron
Template-ID	Uniek nummer	gewoon	ja	automatisch door systeem
User-ID	Intern nummer	gewoon	ja	automatisch door systeem

Naam tabel: Administrator

Attribuut	Omschrijving	type	Verplicht	Bron
ID	Uniek nummer	gewoon	ja	automatisch door systeem
Naam administrator	Accountnaam tbv inloggen van applicatie	gewoon	ja	administrator
Taalcode	Taal waarin de applicatie getoond wordt	gewoon	ja	administrator
Rol	Specificeert de rechten van administrator	gewoon	ja	administrator
Emailadres	Emailadres voor wachtwoordherstel	gewoon	nee	administrator
Wachtwoord	Wachtwoord tbv toegang applicatie[3]	gewoon	ja	administrator

Naam tabel: Template administrator

Attribuut	Omschrijving	Type	Verplicht	Bron
ID	Uniek nummer	gewoon	ja	systeem
Administrator-ID	Verwijzing naar tabel administrator	gewoon	ja	systeem

[2] Het systeem genereert een automatische startdatum en einddatum

[3] Het wachtwoord moet voldoen aan vereisten. Standaard zijn de hoogste eisen ingeregeld. En is het periodiek wijzigen van het wachtwoord verplicht (standaard 1 x per maand). Bij 3 onjuiste pogingen wordt het account van de administrator geblokkeerd gedurende 24 uur.

Template	Gecodeerde string van de vingerherkenningspunten[4]	bijzonder	ja	automatisch door systeem
Omschrijving	b.v. rechter wijsvinger	gewoon	nee	administrator

Naam tabel: Modules

Attribuut	Omschrijving	type	Verplicht	Bron
ID	Uniek nummer	gewoon	ja	systeem
Omschrijving	Naam scanner	gewoon	ja	administrator
Type scanner	Kaartlezer/vingerlezer/gezichtslezer /code tableau	gewoon	ja	administrator
Serienummer	Uniek nummer scanapparaat	gewoon	ja	administrator
Type gebruik	Tijdregistratie j/n, toegangscontrole j/n	gewoon	ja	administrator
Locatie-ID	Locatie-ID van scanner	gewoon	ja	systeem
IP-adres	IP-adres scanner	gewoon	ja	administrator
Poortnummer	TCP-poort scanner	gewoon	ja	administrator
Deur	Locatie waar scanner is geplaatst	gewoon	ja	administrator
Relay Active	Deurschakeling actief j/n	gewoon	ja	administrator
Scanner type	Producent van scanner	gewoon	ja	administrator
Parent ID	Als master-slaveverhouding tussen scanners	gewoon	nee	administrator
Subnetmask	Netwerkinstelling	gewoon	ja	administrator
Serienummer slave	Als master-slaveverhouding tussen scanners	gewoon	nee	administrator
In-out type	Bepaald of er een in of out event plaatsvind	gewoon	nee	administrator
Exit button	Toets voor schakeling deur j/n	gewoon	nee	administrator

3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.

1. Registreren, aanmaken administrator
2. Registreren, aanmaken gebruiker
3. Gebruik IdentySoft voor toegang

Proces 1: Registreren, aanmaken administrator

Stap 1: activeren menu administrators
Aanklikken menu administrators en vervolgens een keuze maken voor toevoegen. Daarna worden de vereiste velden ingevoerd.

Stap 2: wachtwoord en overige gegevens toevoegen
Wachtwoord genereren per administrator. Optioneel ook een email adres invoeren voor wachtwoordherstel en de taal selecteren waar deze administrator mee gaat werken.

Stap 3: rollen toekennen
Rol toekennen aan administrator. Een rol geeft aan wat deze administrator mag zien en beheren binnen de software applicatie.

Stap 4: opslaan aangemaakte gegevens.
Opslaan gegevens

Proces 2: Registreren, aanmaken gebruiker

Stap 1: activeren menu gebruikers
Aanklikken menu gebruikers en vervolgens een keuze maken voor toevoegen.
Daarna worden de vereiste velden ingevuld.

Stap 2: identificatiemiddel toekennen
Aanmaken per gebruiker van de ID-card, toegangscode en/of vingertemplate.

Stap 2: groep/rollen toekennen
Aanmaken per gebruiker van de ID-card, toegangscode en/of vingertemplate.

Stap 3: opslaan aangemaakte gegevens
Opslaan gegevens tbv hergebruik.

Stap 4: synchroniseren met scanners
Opgeslagen wijzigingen worden doorgestuurd naar aangesloten apparaten.

Proces 3: Gebruik IdentySoft voor toegang

Stap 1: plaatsen identificatiemiddel
Plaats uw gezicht voor de scanner.

Stap 2: identificatie
Het systeem zal de gezicht-template herkennen en de toegangsrechten controleren. Afhankelijk van de scanner en toegangsgroep van de gebruiker zal de poort openen.

Stap 3: registratie
Log gegevens van deze actie worden opgeslagen in de software applicatie. De software slaat op wanneer welke gebruiker gebruik heeft gemaakt van het zwembad. Na het uitchecken worden de gegevens gelijk verwijderd.

4. Verwerkingsdoeleinden

Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.

De doelen waarvoor deze persoonsgegevens worden verwerkt zijn:
- het zo efficiënt mogelijk vormgeven van de bedrijfsvoering, zodat tijdig en correct deze gegevens kunnen worden verwerkt.
- naast efficiëntie is beveiliging van de eigendommen een relevant doel, immers diefstal of vernieling schaadt de onderneming.
- ook beveiliging van personen, in geval van calamiteiten, is een belangrijk doel van de registratie van toegang en aanwezigheid. Er moet immers uitsluitsel gegeven kunnen worden of en hoeveel personen zich nog op een locatie bevinden.

Om deze reden heeft Vakantiepark de Witte Berg besloten om IdentySoft te gaan gebruiken als toegangssysteem. Daarmee wordt een grotere mate van nauwkeurigheid bereikt als het gaat om de veiligheid bij calamiteiten. Maar ook is er een betere controle mogelijk op de toegang voor het zwembad.

Voor ondernemers betekent de software gemak bij het bewaken van de toegang tot bedrijfslocaties, voorraden en veiligheid van personeel en goederen. Daarnaast is het in geval van calamiteiten beter te overzien of er nog mensen op locatie zijn of niet.

5. Betrokken partijen

Hier wordt weergegeven welke organisaties betrokken zijn bij de gegevensverwerkingen. Voor elke organisatie is aangegeven in welke rol zij verwerken. Ook de functies binnen een organisatie zijn weergegeven.

Partij	Rol	Functionarissen met toegang tot de (persoons)gegevens
EasySecure	Leverancier IdentySoft als verwerker	Ontwikkelaars updates van software voor beheerstaken.
Vakantiepark de Witte Berg	Verwerkingsverantwoordelijke	Administrator voor inrichting en een beperkt aantal gebruikers
Vakantiepark de Witte Berg	Verwerker voor X voor het planningssysteem	Uitsluitend gepseudonimiseerde gegevens worden doorgegeven

6. Belangen bij de gegevensverwerkingen

Per partij wordt kort de belangen bij de verwerkingen beschreven.

Partij	Belang bij gegevensverwerking
Ondernemer	Veilige en efficiënte bedrijfsvoering
Gasten	Eenvoudige toegang tot het zwembad

7. Verwerkingslocaties

In welke landen vinden de voorgenomen gegevensverwerkingen plaats.

Vraag: Wat wordt in welk land verwerkt uit welk systeem? Ook als er buiten de EER en aangewezen adequate landen wordt verwerkt (Standard contractual clauses op grond van artikelen 44 en 46 AVG).

Antwoord: In Nederland, maar in ieder geval binnen de EU (niet UK).

8. Technieken en methoden van de gegevensverwerkingen

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi) geautomatiseerde besluitvorming, proflering of big data verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

Er is geen semi-geautomatiseerde besluitvorming van toepassing.

Het gaat om cloud software (IdentySoft) voor toegangscontrole, tijd- en/of aanwezigheidsregistratie. Het systeem bestaat uit cloud software, een lokale service en aangesloten scanners.

De IdentySoft software is te benaderen via het internet. De geïnstalleerde service zorgt voor beveiligde communicatie met de cloud. De toegang is dan ook alleen maar te beheren binnen het eigen beveiligde netwerk.

De aangesloten scanners zorgen voor registratie met pas, tag, code of eventueel vinger-templates. Deze scanners sturen toegangsdeuren aan of starten de tijd en aanwezigheidsregistratie. Na identificatie worden de registraties verwerkt in de software.

IdentySoft wordt gehost in de datacenters van Cyso. Cyso is zowel ISO 20000, ISO 27001 en NEN 7510 gecertificeerd. De IdentySoft servers zijn verdeeld over 3 geografisch gescheiden tier4 datacenters in Nederland.

De standaard security updates op deze systemen worden altijd bijgehouden en er wordt direct actief ingegrepen op het moment dat er zich incidenten voordoen. De events op de IdentySoft servers worden 24x7 gemonitord. Er is een doorlopende check op security en een doorlopende check op infrastructuur.

Elke update van de software gaat via een vast traject van ontwikkeling, kwaliteit controle en externe security controles.

Door gebruik te maken van application firewalls en intrusion detection/prevention systems kunnen de servers zeer gedetailleerd gecontroleerd worden op de inhoud van het verkeer.

Door gebruik van Layer 7 filtering en DPI is het mogelijk om op basis van patronen malafide dataverkeer te detecteren en blokkeren. Ook is mogelijk om hiermee de inhoud van het dataverkeer te controleren.

Als een gebruiker heeft gekozen voor registratie met biometrie dan zullen er nooit vingerafdrukken worden opgeslagen. IdentySoft maakt gebruik van een algoritme. IdentySoft scant een vingerafdruk die al in de scanner wordt omgevormd tot een template. Deze template is de uitkomst van een algoritme en bestaat uit 364 posities. Naast dat het algoritme gepatenteerd is, is het ook nog beveiligd met encryptie AES256. Templates zijn niet te herleiden tot een echte afdruk.

Naast de AES256 encryptie maken de scanners ook gebruik van MD2 Hash algoritmes.

9. Juridisch en beleidsmatig kader

Welke wet- en regelgeving is van toepassing. Bijvoorbeeld de AVG, maar ook andere wetgeving kan toepasselijk zijn.

De volgende wet en regelgeving heeft betrekking op de verwerkingen van persoonsgegevens zoals omschreven in voorliggende Data Protection Impact Assessment:

- Algemene verordening gegevensbescherming (AVG);

10. Bewaartermijnen

Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

Gebruikersgegevens: Het bewaartermijn van de gegevens loopt totdat gasten bij ons uitchecken. Na het uitchecken zullen de gegevens omtrent gezichtsherkenning gelijk worden verwijderd.

B. Beoordeling rechtmatigheid

Dit onderdeel gaat over de rechtsgrond, noodzaak en doelbinding van de voorgenomen gegevensverwerkingen en rechten van de betrokkene.

11. Rechtsgrond

Op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

Als rechtsgrond (uit de AVG) komt zowel de toestemming als het gerechtvaardigd belang in aanmerking. De gast kan kiezen (vrijelijk) voor het gebruik van een fysieke toegangsmogelijkheid. Met die keuze, omdat de gast ook echt een keuze heeft, geeft gast toestemming.

De gegevens als zodanig worden niet voor commerciële belangen verder verwerkt.

12. Bijzondere persoonsgegevens[5]

Als er bijzondere, gevoelige of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dit is toegestaan.

Er worden geen bijzondere of gevoelige gegevens verwerkt, anders dan de eerste keer dat men de scanner gebruikt.

13. Doelbinding

Als de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

De gegevens worden niet voor andere doelen gebruikt of hergebruikt dan die eerder in deze DPIA in hoofdstuk 4 zijn beschreven.

14. Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden? Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt? Benoem hierbij de overwogen alternatieven.

De verwerkingen van persoonsgegevens zoals uitgewerkt in deze DPIA worden uitgevoerd voor de doelstellingen zoals omschreven in hoofdstuk 4. Deze verwerkingen van persoonsgegevens zijn gebaseerd op de toestemming van gasten. Op basis van het

[5] Bijzondere gegevens zijn: gegevens over ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap vakbond, genetische gegevens, biometrische gegevens met het oog op unieke identificatie van een persoon, gezondheidsgegevens, seksueel gedrag of gerichtheid.

voorgaande kan worden geconcludeerd dat de verwerkingen van persoonsgegevens noodzakelijk en evenredig zijn.

15. Rechten van de betrokkenen

Hoe wordt invulling gegeven aan de rechten van de betrokkenen. Als de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzondering dat is toegestaan.

Recht op informatie:
Bij het registreren van (gegevens en systeem) dient aan de betrokkene te worden gecommuniceerd waarom deze gegevens worden vastgelegd, voor welke doeleinden en door wie (invulling artikel 13 AVG). Op de website van Vakantiepark de Witte Berg zal zowel voor als tijdens het registratieproces worden verwezen naar de privacyverklaring van Vakantiepark de Witte Berg en Easy Secure.

Recht van inzage en recht van rectificatie:
Vakantiepark de Witte Berg dient het recht van inzage en recht op correctie te faciliteren. Dat is mogelijk via een verzoek aan het management team van Vakantiepark de Witte Berg.

Recht van gegevenswissing:
De gegevens zoals omschreven in deze DPIA worden verwerkt op basis van toestemming en gerechtvaardigd belang. Zolang invulling wordt gegeven aan de bewaartermijnen, is individuele uitvoer van het recht op gegevenswissing niet per definitie nodig. EasySecure zal indien nodig op individueel niveau de uitvoering van dit recht ondersteunen. Vakantiepark de Witte Berg zal de belangen tegenover elkaar afwegen.

Recht op beperking van de verwerking:
De gegevens zoals omschreven in deze DPIA worden verwerkt op basis van toestemming en gerechtvaardigd belang.

Recht op overdraagbaarheid van gegevens:
De gegevens zoals omschreven in deze DPIA worden verwerkt op basis van toestemming en gerechtvaardigd belang. Het recht op overdraagbaarheid van gegevens kan gehonoreerd worden.

Recht van bezwaar:
De persoonsgegevens worden verwerkt op grond van toestemming en gerechtvaardigd belang. Bezwaar is in beginsel altijd mogelijk, bijvoorbeeld in geval van intrekking van de toestemming omdat een medewerker bij nader inzien toch liever gebruik wil maken van een fysieke toegangsmogelijkheid.

Recht om niet te worden onderworpen aan geautomatiseerde besluitvorming:
Niet van toepassing. Er is geen sprake van geautomatiseerde besluitvorming zoals bedoeld in artikel 22 van de Algemene verordening gegevensbescherming.

C. Risico's

Hierna volgen de risico's van de voorgenomen gegevensverwerkingen voor de rechten van betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de voorgenomen gegevensverwerkingen.

16. Risico's

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Ga in ieder geval in op:

a. Negatief gevolg: welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;
b. Oorsprong: de oorsprong van deze gevolgen;
c. Waarschijnlijkheid: de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
d. Ernst: de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

ID	Oorsprong	Negatief gevolg	Waarschijnlijkheid	Ernst
R1	Verloren/gestolen toegangskaart	Mogelijke identiteitsfraude	midden	Afhankelijk van of de verloren/gestolen kaart gebruikt kan worden voor identiteitsfraude. Als ja, dan kunnen de gevolgen heel ernstig zijn. Als nee, dan is de ernst gering.
R2	Afgekeken toegangscodes	Onrechtmatige toegang fysiek	laag	Risico voor medewerker als iemand met die toegangscode fraude pleegt
R3	Wachtwoord wordt afgekeken/gevonden	Onrechtmatige toegang tot systeem	laag	Afhankelijk van de autorisatie van de eigenaar van het wachtwoord
R4	Niet direct verwijderen/blokkeren van gebruikers die uit dienst zijn gegaan	Mogelijk onrechtmatige toegang, autorisatie niet op orde	gemiddeld	Afhankelijk van het autorisatieniveau van medewerker.
R5	Onjuiste autorisaties toekennen	Onbevoegde en mogelijk onrechtmatige toegang. Of geen toegang terwijl dit wel noodzakelijk is.	laag	Afhankelijk van het gewenste autorisatieniveau
R6	Vernieling scanner	Geen toegang of verstoorde toegang	laag	Productieverlies
R7	Software onbereikbaar door internetstoring	Geen inzage in gegevens, geen mutaties mogelijk	laag	Tijdelijk geen inzage in gegevens, mutaties mogelijk. Geen data naar derden. Registratie blijft mogelijk.

D. Maatregelen

Beschrijf de voorgenomen maatregelen om de hiervoor beschreven risico's van de voorgenomen gegevensverwerkingen voor de vrijheden en rechten van de betrokkenen aan te pakken.

17. Maatregelen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden genomen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

ID	Maatregel	Risico	Restrisico	Verantwoordelijke	Status
M1	Blokkeren van de toegangskaart	R1	Geen	Management team Vakantiepark de Witte Berg	
M2	Automatisch verwijderen inactieve gebruikers instellen	R1, R2	Pas/code nog tijdelijk actief	Management team Vakantiepark de Witte Berg	

Toelichting:

- Onder verantwoordelijke is aangegeven wie verantwoordelijk is voor de implementatie van de maatregel.

E. Doorlopende controle

Beschrijf eventuele wijzigingen met betrekking tot de voorgenomen verwerking – bijvoorbeeld de implementatie van een maatregel die voortvloeit uit onderdeel D – om wijzigingen met betrekking tot de verwerking en de mogelijke risico's voor de rechten en vrijheden van natuurlijke personen in kaart te houden.

18. Wijzigingen

Beschrijf mogelijke wijzigingen met betrekking tot de verwerking zoals geïdentificeerd in de voorgaande onderdelen. Dit kunnen wijzigingen zijn die voorgenomen maatregelen implementeren en daarmee een risico adresseren of wijzigingen die een nieuw risico introduceren. Ga hierbij in op:

a. Wijziging: de wijzigingen van de verwerking;
b. Impact risico: of het een bestaand risico adresseert of een nieuw risico introduceert;
c. Referentie: een referentie van de wijziging (indien van toepassing)
d. Datum: de datum waarop de wijziging heeft plaatsgevonden / geldt.

Wijziging	Impact op risico	Referentie	Datum
2FA implementeren in Q1 2020 (2 factor authenticatie)	R3	R3	31-03-2022