Contactless Technologies B.V.
t.a.v. Ruud Peeters
Keizersveld 50
5803 AN Venray

Amsterdam, 31 augustus 2020,

Geachte heer Peeters, beste Ruud,

Recent heeft Contactless Technologies B.V. een nieuwe dienst gelanceerd onder de naam Bank2Loyalty. In de ontwikkelfase die hieraan voorafging kwamen een aantal juridische vragen naar voren. Na een voorgesprek heeft u ons verzocht om onderzoek te doen naar de volgende vraag:

> *Zijn er juridische bezwaren om betaalpassen en mobile wallets ("betaalmiddelen") in te zetten ten behoeve van de dienst Bank2Loyalty, door gebruikers de mogelijkheid te bieden om deze betaalmiddelen te gebruiken om deel te nemen aan loyaliteitsprogramma's van derden?*

Zoals in dit document uiteen wordt gezet, zien wij geen juridische bezwaren om betaalmiddelen op de voorgenomen wijze in te zetten. Belangrijk is wel dat er hierbij persoonsgegevens worden verwerkt. Contactless Technologies dient daarbij de Algemene Verordening Gegevensbescherming in acht te nemen. Tijdens het door ons uitgevoerde 'Privacy Verified' traject is gebleken dat Contactless Technologies de Algemene Verordening Gegevensbescherming op een zorgvuldige wijze in zijn organisatie heeft geïmplementeerd. Van het Privacy Verified traject ontvangt Contactless Technologies een afzonderlijk certificaat.

Voor nadere informatie ben ik natuurlijk steeds beschikbaar.

Met vriendelijke groet,

Mr. ir. Arnoud Engelfriet
Partner ICTRecht B.V.

ICTRECHT

ICTRecht B.V.
Jollemanhof 12
1019 GW Amsterdam

TELEFOON
020 663 1941

E-MAIL
info@ictrecht.nl

INTERNET
ictrecht.nl

KVK
34216164

BTW
NL822330040B01

IBAN
NL07 RABO 0325 2813 78

LOCATIES

NEDERLAND
Amsterdam
Groningen

BELGIË
Brussel

Achtergrond

Contactless Technologies B.V. (hierna: "**Contactless Technologies**") heeft een nieuwe dienst ontwikkeld onder de naam Bank2Loyalty. Deze dienst biedt aan consumenten de mogelijkheid om een fysieke debet- of creditkaart óf een *mobile wallet* zoals Google Pay of Apple Pay (hierna: "**Betaalmiddel**") te gebruiken als universele loyaliteitspas.

Bank2Loyalty gebruikt een uniek kenmerk van het Betaalmiddel om voor iedere consument een eigen klantnummer te berekenen. In de meeste gevallen wordt hiervoor eenvoudigweg het bijbehorende rekeningnummer gebruikt. Het kenmerk wordt via een TLS-versleutelde verbinding naar een centrale server van Contactless Technologies verstuurd. Het kenmerk zelf wordt eveneens versleuteld voordat deze naar de centrale server wordt verstuurd. Op de server van Contactless Technologies wordt het kenmerk vervolgens *gehasht*, oftewel omgezet in een uniek klantnummer, en vervolgens direct verwijderd.

Om gebruik te kunnen maken van Bank2Loyalty moet de consument online een account aanmaken. Aan dit online account kan de consument naar eigen inzicht één of meerdere Betaalmiddelen koppelen. De meeste Betaalmiddelen kunnen direct via de persoonlijke online omgeving van de consument worden gekoppeld. Om andere betaalmiddelen (zoals Google Pay en Apple Pay) te koppelen, dient de consument deze eenmalig te registreren via de Bank2Loyalty reader in één van de aangesloten winkels.

Nadat het Betaalmiddel aan het account gekoppeld is, kan de consument deze in alle aangesloten winkels gebruiken om deel te nemen aan loyaliteitsprogramma's. Het rekeningnummer (of ander kenmerk) wordt niet aan de winkelier of aanbieder van het loyaliteitsprogramma verstrekt. Bank2Loyalty verstrekt aan hen uitsluitend de gegevens die nodig zijn in het kader van het aangeboden loyaliteitsprogramma.

Vraagstelling

Gedurende de ontwikkelfase van Bank2Loyalty kwamen een aantal juridische vragen naar voren. Contactless Technologies heeft ons verzocht om onderzoek te doen naar de volgende vraag:

> *Zijn er juridische bezwaren om betaalpassen en mobile wallets ("betaalmiddelen") in te zetten ten behoeve van de dienst Bank2Loyalty, door gebruikers de mogelijkheid te bieden om deze betaalmiddelen te gebruiken om deel te nemen aan loyaliteitsprogramma's van derden?*

In dit kader zijn met name twee aspecten van belang. Op de eerste plaats is de vraag of consumenten op grond van hun overeenkomst met bijvoorbeeld een bank of *mobile wallet provider* wel het recht hebben om het Betaalmiddel op deze manier te gebruiken. Op de tweede plaats is van belang of het voorgenomen gebruik van de rekeningnummers (of vergelijkbare kenmerken) verenigbaar is met de Algemene Verordening Gegevensbescherming (hierna "**AVG**").

Contractuele gebruiksbeperkingen

Wanneer een consument gebruik wil maken van een Betaalmiddel, sluit hij daarvoor een overeenkomst met een bank of *mobile wallet provider*. De vraag rijst of deze overeenkomst aan het gebruik van het Betaalmiddel voor Bank2Loyalty in de weg staat. Om hier een onderbouwd standpunt over in te kunnen nemen, hebben wij gekeken naar de voorwaarden van verschillende grote banken (meer specifiek: ING, Rabobank en ABN AMRO) en de grootste aanbieders van *mobile wallets* in Nederland (meer specifiek: Apple Pay en Google Pay). Op basis van onze inventarisatie kunnen de volgende conclusies worden getrokken.

Alle onderzochte banken hebben in hun voorwaarden een voorbehoud opgenomen met betrekking tot de eigendom van de uitgegeven betaalpassen. Als 'eigenaar' kan de bank vervolgens naar eigen inzicht voorwaarden verbinden aan het verdere gebruik daarvan door de consument. In alle onderzochte voorwaarden wordt deze mogelijkheid benut en zijn concrete bepalingen opgenomen over het gebruik van het Betaalmiddel. Deze voorwaarden zijn er echter primair op gericht om te voorkomen dat er via het Betaalmiddel onrechtmatige of ongeautoriseerde betalingen worden verricht. Zo verbieden de onderzochte voorwaarden:

1. Het afgeven van het Betaalmiddel aan derden
2. Het in gebruik geven van het Betaalmiddel aan derden
3. Het verstrekken van beveiligingscodes (zoals de pincode) aan derden

Wij hebben in de onderzochte bankvoorwaarden géén bepalingen gevonden die indruisen tegen de voorgenomen dienstverlening van Contactless Technologies. Wanneer een consument gebruik maakt van Bank2Loyalty wordt enkel een algemeen kenmerk zoals een rekeningnummer uitgelezen. Dit kenmerk wordt *gehasht* en daarna direct verwijderd. Er wordt door Contactless Technologies niet om beveiligingscodes gevraagd. De kans op misbruik is daardoor zeer klein.

Ook in de voorwaarden van de grootste *mobile wallet providers* hebben wij geen voorwaarden gevonden die tegen het door Contactless Technologies voorgenomen gebruik indruisen. De aanbieders van deze *mobile wallets* stellen enkel een aantal algemene beperkingen, zoals leeftijdsbeperkingen. Voor het overige verwijzen zij door naar de voorwaarden van de uitgever van de kaart die in de *mobile wallet* wordt opgeslagen. Contactless Technologies maakt echter een eigen loyaliteitspas aan die in de *mobile wallet* van de consument wordt opgenomen. Er lijken derhalve geen andere relevante voorwaarden die hier een belemmering kunnen vormen.

Privacyrechtelijke aspecten

Zoals hiervoor beschreven, wordt bij de dienstverlening van Contactless Technologies een kenmerk van het Betaalmiddel (meestal het rekeningnummer) verwerkt. De AVG verzet zich als zodanig niet tegen het gebruik hiervan door Contactless Technologies. Van belang is echter wel dat dergelijke gegevens kwalificeren als "persoonsgegevens" onder de AVG. Dat betekent dat Contactless Technologies bij de verwerking van deze gegevens diverse verplichtingen in acht moet nemen. De belangrijkste principes waarmee rekening moet worden gehouden zijn te vinden in artikel 5 van de AVG.

Middels een Privacy Verified traject hebben wij vastgesteld dat Contactless Technologies de hiervoor bedoelde principes uit de AVG zorgvuldig in zijn

organisatie heeft geïmplementeerd. Hieronder wordt kort bij deze principes stilgestaan en worden onze bevinden uit het Privacy Verified traject kort samengevat.

Transparantiebeginsel

Een centraal beginsel in de AVG is het zogeheten transparantiebeginsel. Dit beginsel houdt – kort gezegd – in dat Contactless Technologies de personen waarvan hij persoonsgegevens verwerkt (ook wel "**betrokkenen**") daarover duidelijk moet informeren. Contactless Technologies heeft aan dit beginsel uitvoering gegeven door op zijn website een privacy- en cookieverklaring te plaatsen. Deze verklaring is gemakkelijk te raadplegen voor betrokkenen, zowel voordat zij een account aanmaken voor Bank2Loyalty als nadat zij zich voor de dienst hebben aangemeld. Tijdens het door ons uitgevoerde Privacy Verified traject hebben wij vastgesteld dat de privacyverklaring voldoet aan de eisen die de AVG daaraan stelt.

Doelbindingsbeginsel

Op grond van de AVG mag Contactless Technologies alleen persoonsgegevens verwerken voor duidelijk afgebakende doeleinden. Het primaire doel voor Contactless Technologies om persoonsgegevens te verwerken, is het mogelijk maken van Bank2Loyalty. Contactless Technologies sluit een overeenkomst met betrokkenen die gebruik willen maken van deze dienst en heeft een aantal persoonsgegevens nodig om hieraan uitvoering te kunnen geven. Zo is het voor Contactless Technologies noodzakelijk om een *gehasht* rekeningnummer of vergelijkbaar kenmerk op te slaan in het account van de betrokkene, zodat het bijbehorende Betaalmiddel kan worden herkend in de aangesloten winkels. Zonder een dergelijk (uniek) nummer of kenmerk op te slaan, zou Contactless Technologies niet weten bij welke betrokkene het Betaalmiddel hoort. Het zou dan ook niet mogelijk zijn om loyaliteitspunten of opgebouwde aanspraken aan de juiste betrokkene toe te kennen. Een volledig overzicht van de persoonsgegevens die Contactless Technologies verwerkt, en de doeleinden waarvoor deze gebruikt worden, is opgenomen in de privacy- en cookieverklaring.

Beginsel van dataminimalisatie

Uitgaande van de AVG mag Contactless Technologies niet meer gegevens verwerken dan nodig is gelet op het doel waarvoor de persoonsgegevens worden verwerkt. Contactless Technologies heeft al gedurende de ontwikkeling van Bank2Loyalty rekening gehouden met dit uitgangspunt. Zo wordt het gebruikte identificerende kenmerk van een Betaalmiddel direct *gehasht,* waarna het oorspronkelijke kenmerk wordt verwijderd. Ook heeft Bank2Loyalty velden in het aanmeld- en contactformulier die niet strikt noodzakelijk zijn, maar die wel de dienstverlening ten goede kunnen komen 'optioneel' gemaakt. Betrokkenen kunnen er derhalve zelf voor kiezen of zij deze gegevens wel of niet willen achterlaten.

Beginsel van juistheid

De AVG verplicht Contactless Technologies om zich maximaal in te spannen om te voorkomen dat er onjuiste of onvolledige persoonsgegevens worden verwerkt. Contactless Technologies heeft verschillende maatregelen genomen om dit te voorkomen. De belangrijkste voorzorgsmaatregel die Contactless Technologies heeft genomen, is de ontwikkeling van een online dashboard. Via dit online dashboard kunnen gebruikers van Bank2Loyalty op ieder moment inzien welke

gegevens er van hun zijn geregistreerd, welke Betaalmiddelen er aan hun account zijn gekoppeld en voor welke loyaliteitsprogramma's zij zijn aangemeld. Betrokkenen kunnen hun gegevens via dit online dashboard ook eenvoudig wijzigen als deze onjuist of verouderd blijken te zijn. Op die manier houden betrokkenen grip op hun persoonsgegevens.

Beginsel van opslagbeperking

Contactless Technologies mag persoonsgegevens niet langer bewaren dan noodzakelijk is gelet op het doel waarvoor de persoonsgegevens zijn verkregen. Om dit te voorkomen heeft Contactless Technologies binnen zijn organisatie duidelijke bewaartermijnen vastgesteld. Met de winkels en aanbieders van loyaliteitsprogramma's waarmee Contactless Technologies samenwerkt, zijn contractuele afspraken gemaakt om te voorkomen dat persoonsgegevens onnodig lang door hun worden bewaard. De door Contactless Technologies gehanteerde bewaartermijnen zijn ook opgenomen in de privacy- en cookieverklaring, zodat betrokkenen hier direct inzage in hebben.

Integriteit en vertrouwelijkheid

Contactless Technologies dient op grond van de AVG te zorgen voor een passende beveiliging, zowel op technisch als organisatorisch vlak. In dit kader constateren wij dat Contactless Technologies onder meer de volgende stappen heeft gezet:

- Het gebruik van onveilige wachtwoorden wordt tegengegaan middels unieke eenmalige tokens die de betrokkene per e-mail of sms ontvangt.
- De verbindingen tussen de verschillende onderdelen van Bank2Loyalty worden versleuteld met gebruik van TLS-technologie.
- Verwerkte gevoelige persoonsgegevens (zoals bankrekeningnummers) worden enkel in *gehashte* vorm opgeslagen.
- Er worden logbestanden bijgehouden met betrekking tot het verkrijgen van toegang tot persoonsgegevens.
- De persoonsgegevens worden opgeslagen in sterk beveiligde, professionele datacenters welke ISO/IEC 27001:2013 zijn gecertificeerd.

Contactless Technologies heeft daarmee zowel op technisch als op organisatorisch vlak maatregelen genomen om onrechtmatige toegang tot – of verwerking van – persoonsgegevens te voorkomen.

Conclusie

Op basis van het voorgaande zien wij geen juridische bezwaren om betaalpassen en *mobile wallets* in te zetten ten behoeve van Bank2Loyalty. De voorwaarden van de meest gebruikte banken en *mobile wallet providers*, bevatten geen clausules die dit verbieden. Ook zien wij geen overtuigende argumenten voor deze partijen om dat in de toekomst wel te doen.

Het uitlezen van rekeningnummers of daarmee vergelijkbare kenmerken kwalificeert wel als een "verwerking van persoonsgegevens". Om die reden dient Contactless Technologies zich te conformeren aan de AVG. Middels een 'Privacy Verified' traject hebben wij vastgesteld dat Contactless Technologies de Algemene Verordening Gegevensbescherming op een zorgvuldige wijze in zijn organisatie heeft geïmplementeerd. Hiervan ontvangt Contactless Technologies een afzonderlijk certificaat.