Privacy Statement Multicard Nederland BV

1.1 Inleiding

Beveiliging van data is één van de speerpunten van Multicard Nederland BV, nader te noemen Multicard. Multicard legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens[1] te beveiligen tegen gebruikersfouten, virussen, verlies of tegen enige vorm van ongeoorloofde verwerking. Deze technische en organisatorische maatregelen garanderen, rekening houdend met de stand der techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen. De beveiliging van persoonsgegevens kent drie kwaliteitsaspecten: Exclusiviteit (uitsluitend geautoriseerde personen hebben toegang tot en kunnen gebruik maken van persoonsgegevens), Integriteit (juistheid programmatuur en gegevens) en Continuïteit (beschikbaarheid van netwerken en gegevens). Dit privacy statement geeft beknopt aan op welke wijze Multicard de data van haar klanten beschermt.

1.2 Autoriteit Persoonsgegevens & AVG

Multicard personaliseert informatiedragers en verzorgt en beheert datastromen. De (persoonlijke) gegevens die benodigd zijn voor het personalisatieproces en de datastromen worden verkregen van/via klanten. Multicard is dan ook verwerker[2] van de gegevens.

De algemene verordening gegevensbescherming geeft regels voor het verwerken van persoonsgegevens. De AVG is op 25 mei 2018 in werking getreden. De belangrijkste privacy speerpunten zijn:

- Multicard raadpleegt en verwerkt alleen persoonsgegevens als dit noodzakelijk is voor de realisatie van een specifiek en vooraf vastgesteld doel.
- Multicard verwerkt nooit meer gegevens dan noodzakelijk is en bewaart de persoonsgegevens niet langer dan noodzakelijk.
- Iedereen binnen Multicard is persoonlijk verantwoordelijk voor een zorgvuldige omgang met persoonsgegevens en de beveiliging ervan in overeenstemming met de privacy beleidstukken en richtlijnen.
- Binnen Multicard wordt continue gewerkt aan de privacy awareness van medewerkers door awareness materialen en de inzet van de Functionaris Gegevensbescherming. Privacy is een vast agendapunt in de periodieke overlegstructuren.
- Elk beveiligingsincident waar (mogelijk) persoonsgegevens bij zijn betrokken wordt direct na constatering gemeld bij het Meldpunt Incidenten.
- Multicard is transparant over de wijze waarop zij persoonsgegevens verwerkt en over de rechten die betrokkenen kunnen uitoefenen.
- Klanten hebben de mogelijkheid om controle over hun persoonsgegevens uit te oefenen.
- Multicard vraagt de klant voor de start van de verwerking om (ondubbelzinnige) toestemming als zij geen beroep kan doen op een andere wettelijke grondslag.

Meer informatie over de AVG is te vinden op: **www.avg.nl**.

[1] Zie voor uitleg persoonsgegevens, verklaring begrippen
[2] Zie voor uitleg verwerker, verklaring begrippen

1.3 Fysieke beveiliging en omgevingsbeveiliging

Het pand van Multicard is Klasse 4 (verzekeringsnorm) beveiligd en voorzien van camera's, die 24/7 opnames maken. Daarnaast zijn onderstaande veiligheidsmaatregelen opgenomen:

- Het pand is voorzien van inbraakalarm en aangesloten op een meldkamer;
- De passen staan in brandvertragende kluizen opgeslagen;
- De printafdeling is als apart compartiment extra beveiligd door middel van rolluiken;
- Alle afdelingen zijn alleen bereikbaar voor daartoe geautoriseerde medewerkers. Alle entries worden gelogd;
- Alle servers van Multicard staan in geconditioneerde, afgesloten ruimten.
- Het bedrijventerrein waarop Multicard zich bevind is collectief beveiligd.

1.4 Softwarematige beveiligingen

Multicard software, SAAS worden beheerd door Yaguti Systems hosting service met het gebruik van Microsoft Technologies Virtualization Platforms en High-End Data Center Capabilities in Rotterdam, deze zijn direct verbonden aan de Internet Exchange. Het platform heeft de volgende certificaten en voldoet aan de Algemene verordening gegevensbescherming (AVG). ISO9001:2015, ISO14001:2015, NEn7510:2017 (De eerste partij in Nederland tegen de nieuwe norm gecertificeerd) en ISO27001:2013

Naast het feit dat de systemen van Multicard in een professioneel beveiligde omgeving staan is de toegang tot de software waarin de informatie wordt opgeslagen (o.a. Yoonidata/Mybility/Mycashless) ook beveiligd door de volgende maatregelen:

- Alle computerapparatuur en netwerkfaciliteiten zijn afgeschermd door middel van logische toegangsbeveiliging;
- Alle medewerkers hebben een persoonlijke toegangscode met wachtwoord, die hen alleen toegang geeft op van te voren geautoriseerde niveaus;
- Alle handelingen binnen Yoonidata, Mybility en Cashless Betalen worden gelogd;
- Alle gegevens die elektronisch verzonden worden, zijn versleuteld;
- Voor alle webbased applicaties van Multicard wordt er gebruikgemaakt van SSL certificaten[3];
- Multicard werkt met Firewall[4] hard- en software en met antivirus software[5];
- Indien gewenst geeft Multicard accountverklaringen af.

1.5 Continuïteit opslag persoonsgegevens

Dagelijks worden op vaste tijdstippen, back-ups gemaakt van systemen. De gevoeligheid voor storingen en calamiteiten wordt hierdoor beperkt. Het maken van back-ups met persoonsgegevens zijn in duidelijke procedures vastgelegd, waarvan de naleving wordt gecontroleerd. Voor het waarborgen van de continuïteit van de verwerking van persoonsgegevens worden de back-ups in een inbraak werende ruimte (kluis) bewaard. Deze ruimte, of de omgeving waarin deze zich bevindt, is voorzien van extra inbraakdetectie. De back-ups worden allemaal ook buiten het gebouw van Multicard bewaard.

1.6 Vernietigen persoonsgegevens

Indien er gewerkt wordt met gepersonaliseerde formulieren, dan worden deze na gebruik, indien ze niet teruggaan naar de klant, aangeboden bij een gecertificeerde archiefvernietiger en niet bij reguliere papierafval gestort. Ook uitvalpassen worden vernietigd.

[3] Zie voor uitleg SSL certificaat, verklaring begrippen
[4] Zie voor uitleg Firewall, verklaring begrippen
[5] Zie voor uitleg antivirus, verklaring begrippen

2 Verklaring begrippen

2.1 Wat zijn persoonsgegevens in het kader van de AGV?

Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

2.2 Wat is een verwerking?

Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

2.3 Wie is de verwerkingsverantwoordelijke?

Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lid statelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen

2.4 Wie is de verwerker?

Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

2.5 SSL certificaat

Een SSL certificaat beveiligt de verbinding tussen uw klant en uw website. Het certificaat zorgt voor de encryptie van de verbinding, en voor het valideren van de identiteit van uw website. Met behulp van een SSL Certificaat is uw bezoeker er zeker van dat hij op uw website is gekomen, en dat de door hem ingevoerde gegevens niet door derden kunnen worden afgeluisterd. Een SSL Certificaat is noodzakelijk voor elke website waarbij privacy gevoelige gegevens zoals creditcard gegevens en wachtwoorden worden uitgewisseld.

2.6 Data uitwisseling

Wanneer het gaat om data-uitwisseling via een directe koppeling maken wij gebruik van WebServices, gebaseerd op XML of JSON (REST), gebruik makend van SSL. Authenticatie wordt afgestemd met de ontvanger of zender. Dit kan via Oauth, servercertificaten en in sommige gevallen nog met een gebruikersnaam en wachtwoord (Basic Authentication), al implementeren we het laatste niet meer voor nieuw te ontwikkelen koppelingen. Wanneer data via FTP wordt verstuurd, maken wij (met instemming van de klant) gebruik van SFTP of FTPS.

2.7 Firewall

Firewall is letterlijk vertaald in het Nederlands 'brandmuur'. Dit soort muren (in gebouwen toegepast) dient om te voorkomen dat een brand aan de ene kant van de muur overslaat naar de andere kant.

Op dezelfde manier heeft een firewall in een computernetwerk tot doel te voorkomen dat ongewenst verkeer van de ene netwerkzone terecht komt in een andere, teneinde de veiligheid in de laatstgenoemde te verhogen. Het ongewenste verkeer bestaat bijvoorbeeld uit aanvallen van *hackers*.

2.8 Antivirus software

Antivirus software is software die e-mailverkeer scant op computervirussen, spyware en spam.