white paper

Resono security en privacybeleid



Door:
Frank Verschoor
Remco Bron

Datum: maart 2022
Versie: 2022.4.0

Foto Jenny Ueberberg

1. Introductie

Resono Benchmark geeft de direct en doorlopend inzicht in drukte en bezoekersgedrag op en in fysieke locaties. De data hiervan wordt verzameld via een wijdverspreid panel aan smartphone apps. Gebruikers van deze apps hebben toestemming verleend voor het anoniem verzamelen van locatiegegevens.

2. Resono Mobile Panel

Het Resono mobile panel is opgebouwd vanuit apps waarbij de Resono SDK is geïntegreerd. Deelnemende apps stellen bereik beschikbaar zodat Resono volstrekt anoniem locatiegegevens kan aggregeren.

Aan gebruikers die toestemming verlenen wordt binnen het Resono platform een eigen device-ID toegekend dat alleen door Resono wordt gebruikt. Dit Resono-ID wordt alleen ter identificatie van het device gebruikt en bevat geen verdere persoonlijke kenmerken. Het Resono-ID wordt alleen intern gebruikt voor de uitvoering van sommige aggregaties en wordt nooit gedeeld met derden.

3. Gebruiker opt-in / opt-out

Aan iedere gebruiker van deze apps is expliciet toestemming gevraagd voor het gebruik van locatiegegevens. Hierbij wordt melding gemaakt dat deze voor analytische en marketingdoeleinden voor derden kunnen worden gebruikt. Resono wordt hierbij benoemd bij de opt-in als verwerker van deze data met een link naar de privacy statement van Resono. Alleen indien een gebruiker toestemming heeft gegeven kan Resono deze gegevens benutten. Zonder toestemming wordt geen enkel gegeven van de gebruiker vastgelegd.

Het betreft een opt-in technologie waarbij de gebruiker op ieder gewenst moment toestemming kan geven of intrekken voor het gebruik van locatiegegevens.

3.1 iOS opt-in flow

1) App wordt geïnstalleerd door gebruiker.
2) Bij de eerste keer opstarten van de app krijgt de gebruiker de vraag voor toestemming tot locatie. Hierbij wordt in de toelichting vermeld dat de locatie voor marketing en analytische doeleinden wordt gebruikt en is er een link naar de privacy statement van Resono..
    a) Bij akkoord ontvangt Resono nog geen locatie data
    b) Bij geen akkoord of één sessie ontvangt Resono nooit locatiedata

3) Na 10 tot 24 uur van de app installatie (door iOS zelf bepaald) krijgt de gebruiker de vraag of de locatie altijd op de achtergrond gebruikt mag worden.
    a) Bij akkoord ontvangt Resono locatiedata
    b) Bij geen akkoord Resono nooit locatiedata
4) Meerdere malen op willekeurige tijden (door iOS bepaald) moet de gebruiker nogmaals toestemming geven voor gebruik van locatie op de achtergrond.
    a) Bij akkoord ontvangt Resono locatiedata
    b) Bij geen akkoord Resono nooit locatiedata

3.2 Android opt-in flow

1) App wordt via de Google Play store geïnstalleerd door de gebruiker
2) bij de eerste keer opstarten van de app krijgt de gebruiker de vraag of de app toegang tot de locatie van het apparaat mag hebben. Hierbij wordt in de toelichting vermeld dat de locatie voor marketing en analytische doeleinden wordt gebruikt door Resono met een link naar de privacy statement van Resono.
    a) Bij toestaan ontvangt Resono locatie data
    b) Bij weigeren ontvangt Resono nooit locatie data

3.3 Opt-out (iOS en Android)

Bij de privacy instellingen op het device kan de gebruiker altijd de toestemming tot locatiegegevens deactiveren in zijn geheel of vaak ook per derde partij. Bij deactivatie kan de app nog wel worden gebruikt maar ontvangt Resono geen locatiedata. Op het moment dat de locatie toestemming wordt ingetrokken zijn binnen 36 uur alle locatiegegevens van dit device bij Resono verwijderd. Dit werkt automatisch.

4. Privacydrempel

Niet iedere gebruiker is onderdeel van het Resono mobile panel. Daarmee vormen de gegevens dus een steekproef. Resono berekent met Benchmark op basis van deze steekproef een zo accuraat mogelijke schatting van het gedrag van een een grotere populatie.

Welke gegevens in de berekening worden opgenomen is afhankelijk van ze de door Resono gestelde privacydrempel behalen. De privacydrempel is bedoeld om ten alle tijde anonimiteit van individuele gebruikers te waarborgen. Wanneer de privacydrempel niet wordt behaald rapporteert Resono deze gegevens niet.

5. Differentiële privacy

Resono maakt direct na het verzamelen van de gegevens gebruik van differentiële privacy, dat wil zeggen dat er kunstmatige ruis aan de datasets wordt toegevoegd direct na ontvangst van de data. Zo kunnen resultaten van hoge kwaliteit worden gegenereerd zonder dat deze data herleidbaar is tot een individu, ook niet door Resono zelf.

Deze privacy beschermende maatregelen zorgen er ook voor dat het absolute aantal bezoeken nooit bekend wordt gemaakt en alleen geaggregeerde gegevens worden gerapporteerd. Deze technologie wordt breed toegepast door partijen als Apple en Google om privacy van gebruikers te garanderen. UC Berkeley Center for Long-Term Cybersecurity heeft hierover een interessante uitlegvideo gepubliceerd: https://youtu.be/NRf6sUk1bv0
Resono past differential privacy toe met een epsilon van 8.

6. Data aggregatie

De rapportages die Resono levert aan haar klanten betreft alleen geaggregeerde data voor statistische doeleinden (bijvoorbeeld aantal bezoekers per dag in een winkel) die op geen enkele wijze herleidbaar is naar een individuele gebruiker.

Per rapport wordt steeds van een andere aggregatie gebruik gemaakt om te kunnen voldoen aan de privacyregels. De kruisbezoeken rapportage is bijvoorbeeld niet per kwartier beschikbaar en de kwartiergegevens bevatten geen kruisbezoek. De aggregatie wordt steeds aangepast volgens de eis dat er voldoende niveau van anonimiteit bereikt dient te worden.

Resono data voldoet daarmee volledig aan ‘statistische geheimhouding’ volgens GDPR/AVG verordening 162: http://www.privacy-regulation.eu/nl/r162.htm

7. Bewaartermijn

De anonieme locatiegegevens van het Resono mobile panel worden niet langer dan noodzakelijk opgeslagen, met een maximale bewaartermijn van 3 maanden. Deze bewaartermijn wordt gehandhaafd om correcties op de data achteraf te kunnen doorvoeren.

8. Opslag en dataverwerking

8.1 OWASP security controle

Resono controleert alle beveiliging van systemen te allen tijde op basis van de OWASP top-10 lijst. Onderdeel van deze internationaal aanvaarde security maatregelen zijn onder meer XSS (cross-site-scripting), CRSF (cross-site request forgeries) en Code-Injection checks.

8.2 Beveiligde communicatie tussen systemen

De communicatie tussen smartphones en Resono verloopt via SSL en is versleuteld via up-to-date TLS. De RSA Certificatie Autoriteit heeft Resono het RSA Domain Validation Secure Server certificaat verstrekt, dat van toepassing is op de encryptie van de communicatie. Tevens wordt om spoofing te voorkomen alle communicatie via Resono API's beveiligd op basis van een accountsecret.

8.3 Toegang tot de server

Alle Resono-servers hebben RSA-sleutels voor toegangscontrole, evenals een optionele twee factor-authenticatie (2FA). Alle wachtwoorden worden gehashed opgeslagen.

8.4 Cloud Hosting

8.4.1 Google Cloud

Resono gebruikt Google Big Query en Google Cloud Storage voor de verwerking en opslag van gegevens. De gegevens worden alleen opgeslagen op servers van de Europese Unie (Regio West-1;Belgie) en West-4;Nederland). Google Cloud zet zich in voor de naleving van de algemene gegevensbeschermingsverordening van de EU (GDPR) voor alle diensten van het Google Cloud-platform. Alle Big Query data wordt versleuteld opgeslagen.

8.4.2 Linode

De overige cloud hosting vindt plaats bij Linode in het datacenter in Frankfurt am Mainz (gecertificeerd volgens ISO 27001) Linode is een wereldwijd top 10 hostingbedrijf en PCI Data Security Standard (PCI DSS) compliant, welke is gevalideerd door een geautoriseerde onafhankelijke Qualified Security Assessor. Door middel van regelmatige scans en evaluaties houdt Linode zich aan de PCI DSS eisen voor veiligheidsmanagement, beleid, procedures, netwerkarchitectuur, software ontwerp en andere kritische beschermingsmaatregelen.

Linode handhaaft strenge filterregels om ervoor te zorgen dat het netwerk alleen met hun toegestane IP-adressen kan communiceren. Dit voorkomt dat IP's van andere Linodes kan spoofen of man-in-the-middle-aanvallen kan uitvoeren op een privé-netwerk.

8.5 Geautomatiseerd testen

Dagelijks voert Resono geautomatiseerde testprocedures uit om de betrouwbaarheid van het platform te valideren (*continuous integration*). Nieuwe versies zijn alleen toegestaan na validatie van deze testprocedures.

8.6 Externe validatie

Alle Resono beveiligingsaspecten zijn getest door onafhankelijk beveiligingsbureau Computest in opdracht van een klant van Resono. Alle aanbevelingen uit dit onderzoek zijn doorgevoerd.

9. Certificeringen

De methodes die Resono hanteert zijn gecertificeerd en voldoen volledig aan alle geldende Europese GDPR en Nederlandse AVG regel- en wetgeving.

Dit is onafhankelijk vastgesteld door ICTRecht in oktober 2021. Resono heeft van ICTRecht de vooraanstaande 'Privacy Verified' extended certificering ontvangen waarmee is vastgesteld dat de methodiek en processen geheel voldoen aan alle wetgeving en AVG richtlijnen.

ICTRecht wordt al jaren vertrouwd op dit gebied door opdrachtgevers als TomTom, Air Miles, Ministerie van Buitenlandse Zaken, Kieskompas, Thuiswinkel.org en Wolters Kluwer.

Deze certificering is een doorlopend proces; bij aanpassingen aan of aanvullingen op methodieken of processen wordt ICTRecht betrokken om zeker te zijn dat dit volgens wet- en regelgeving toegestaan is. Meer informatie hierover is te vinden op https://www.privacyverified.nl/bedrijfscertificering/hoe-het-werkt

Daarnaast is Resono aangesloten bij het IAB Europe Transparency and Consent Framework en bij het Fair Data Keurmerk van het Nederlandse Expertise Center voor Marketing Insights (MOA).

PRIVACY VERIFIED

APPROVED STATUS iab europe Transparency and Consent Framework REGISTERED VENDOR

Fair Data™ PRIVACY IN VERTROUWDE HANDEN

10. Conclusie

Het Resono platform is ontwikkeld volgens het privacy by design principe. Op alle fronten biedt Resono gezamelijk met haar app partners de gebruiker die meewerkt aan het app panel enerzijds strikte anonimiteit en anderzijds de mogelijkheid om na een opt-in altijd te stoppen met medewerking en de mogelijkheid om alle eigen informatie te laten verwijderen van het Resono platform. Daarmee voldoet Resono aan alle Nederlandse AVG en de Europese GDPR wetgeving.

Over de auteurs



Frank Verschoor

privacy officer Resono
frank@reso.no

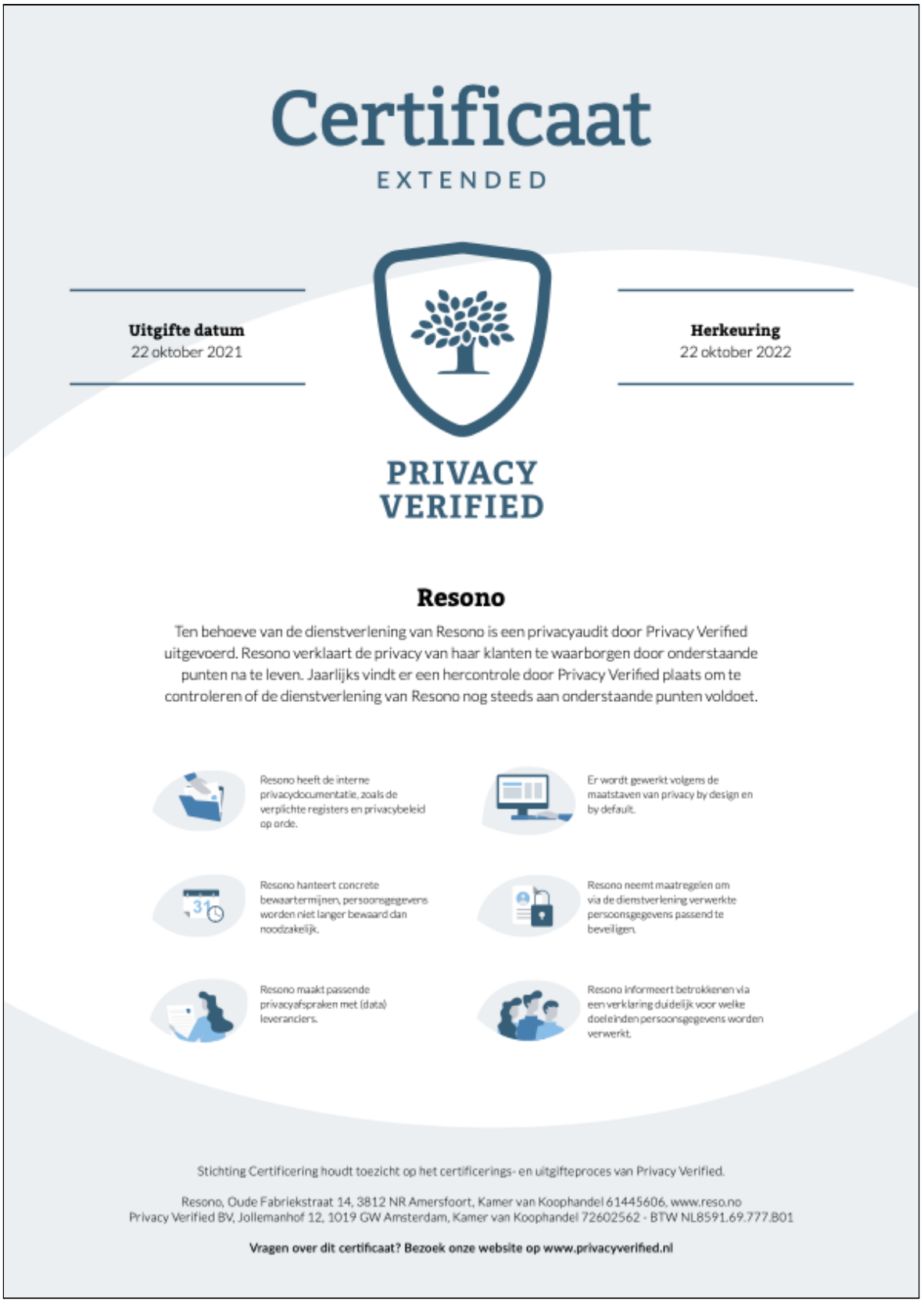
Frank heeft een track record in het ontwikkelen en internationaal in de markt zetten van bedrijven met innovatieve technologie In zijn rol als privacy officer van Resono draagt hij zorg voor het correct uitvoeren van het privacy en security beleid van Resono.



Remco Bron
co-founder & CEO Resono
remco@reso.no

Remco heeft meer dan 20 jaar ervaring met het vinden en implementeren van IT oplossingen binnen organisaties. Hij is verantwoordelijk dagelijkse zaken rondom Resono accounts

Bijlage 1: Privacy Verified Certificaat ICTRecht



Certificaat

EXTENDED

Uitgifte datum
22 oktober 2021

Herkeuring
22 oktober 2022

PRIVACY VERIFIED

Resono

Ten behoeve van de dienstverlening van Resono is een privacyaudit door Privacy Verified uitgevoerd. Resono verklaart de privacy van haar klanten te waarborgen door onderstaande punten na te leven. Jaarlijks vindt er een hercontrole door Privacy Verified plaats om te controleren of de dienstverlening van Resono nog steeds aan onderstaande punten voldoet.

Resono heeft de interne privacydocumentatie, zoals de verplichte registers en privacybeleid op orde.

Er wordt gewerkt volgens de maatstaven van privacy by design en by default.

Resono hanteert concrete bewaartermijnen, persoonsgegevens worden niet langer bewaard dan noodzakelijk.

Resono neemt maatregelen om via de dienstverlening verwerkte persoonsgegevens passend te beveiligen.

Resono maakt passende privacyafspraken met (data) leveranciers.

Resono informeert betrokkenen via een verklaring duidelijk voor welke doeleinden persoonsgegevens worden verwerkt.

Stichting Certificering houdt toezicht op het certificerings- en uitgifteproces van Privacy Verified.

Resono, Oude Fabriekstraat 14, 3812 NR Amersfoort, Kamer van Koophandel 61445606, www.reso.no
Privacy Verified BV, Jollemanhof 12, 1019 GW Amsterdam, Kamer van Koophandel 72602562 - BTW NL8591.69.777.B01

Vragen over dit certificaat? Bezoek onze website op www.privacyverified.nl