Whitepaper

API calls *en GDPR*

Het **synchroniseren** van je CRM-systeem met andere tools via API calls is tegenwoordig een basisvoorwaarde voor een **efficiënte werking binnen je bedrijf.** Of het nu gaat om het koppelen van een e-mailmarketingplatform, ERP-systeem of klantportaal: een naadloze integratie van gegevens **bespaart tijd, voorkomt fouten en optimaliseert processen.**

Zodra er ***persoonsgegevens*** worden gedeeld, kom je echter op het terrein van de ***GDPR*** (ook wel *AVG, voluit Algemene Verordening Gegevensbescherming*). Hoewel de regels op dit terrein intussen al wat duidelijker zijn, blijft de praktische toepassing ervan ***complex.***

Deze whitepaper biedt inzichten en best practices om API-synchronisaties zo in te richten dat ze voldoen aan de principes van GDPR. ***Let op:*** dit document is bedoeld ter informatie en ***vervangt geen juridisch advies.*** Voor specifieke vragen raden we aan contact op te nemen met een juridisch expert.


make it fly

01

Wat zegt GDPR over ***datadeling***

De kern van GDPR:

bescherming van *persoons-gegevens*

De ***GDPR-regelgeving*** is in het leven geroepen om de privacy van individuen binnen de EU te beschermen. Elk stukje informatie waarmee je een persoon kan identificeren - van namen en e-mailadressen tot IP-adressen en klantgedrag - dient strikt beschermd te worden. Bedrijven die deze gegevens verwerken, hebben bijgevolg ***de plicht om dit op een veilige en transparante manier te doen.***

De rol van

API's in gegevens-uitwisseling

API's maken het mogelijk om ***data te delen tussen systemen.*** Een API-call kan zo klantgegevens bevatten die door meerdere systemen worden verwerkt of opgeslagen. Gezien deze klantgegevens vaak te herleiden zijn tot een persoon (namen, e-mailadressen, IP-adressen), is het ***belangrijk om zorgvuldig met API-calls om te springen.***

Bij het synchroniseren

van data via API's heb je *twee rollen*

- ***Verwerkingsverantwoordelijke,*** Je bepaalt welke gegevens worden verzameld en waarom.
- ***Verwerker,*** Je verwerkt gegevens namens een andere partij (bijvoorbeeld een klant).

Bij het synchroniseren

van data via API's heb je *twee rollen*

Bij beide rollen moet je ervoor zorgen dat je aan de GDPR-regelgeving voldoet. ***Dit doe je bijvoorbeeld door een Data Processing Agreement (DPA)*** af te sluiten. Een DPA is een verplichte overeenkomst die wordt afgesloten tussen twee of meer partijen als de ene partij persoonlijke gegevens (van derden) verwerkt voor een andere partij, zoals bijvoorbeeld het geval is in een CRM-systeem.

02

Dataoverdracht *via API calls*

Wat gebeurt er bij een ***api call?***

Een API (Application Programming Interface) is ***een digitale snelweg waarmee systemen met elkaar communiceren.*** Bij een API-call verstuurt systeem A (bijvoorbeeld je CRM), een verzoek naar systeem B (bijvoorbeeld een marketingplatform) om data op te halen, te wijzigen of te verwijderen.

Elke API-call ***kan verschillende gegevenstypes bevatten,*** van simpele tekst tot complexe datapunten zoals persoonlijke klantgegevens. Dit maakt API-'s krachtig, maar ook kwetsbaar.

Risico's
bij een gegevens-overdracht

Zonder encryptie kunnen gegevens worden ***onderschept***

Tijdens de overdracht kan data kwetsbaar zijn voor ***manipulatie of verlies***

Of een configuratiefout, waarbij een verkeerd ingestelde API ***te veel data vrijgeeft of verkeerde ontvangers*** toegang krijgen

Bij elke API-call waarin persoonsgegevens worden uitgewisseld, zijn twee aspecten dus cruciaal: ***versleuteling (encryptie) en authenticatie.*** Deze twee pijlers zorgen ervoor dat gegevens niet alleen ***veilig worden verzonden,*** maar ook dat alleen de ***juiste partijen er toegang toe krijgen.*** We lichten beide aspecten hieronder verder toe.

Bij encryptie worden de gegevens ***versleuteld*** verzonden (via HTTPS of TLS). Zo wordt data ***onleesbaar*** gemaakt voor iedereen die ***niet de juiste toegang heeft***, om te voorkomen dat mensen met verkeerde bedoelingen gevoelige gegevens kunnen onderscheppen tijdens de overdracht tussen systemen.

Authenticatie ***voorkomt dat onbevoegde gebruikers of systemen toegang krijgen*** tot je API en de gegevens die worden uitgewisseld. Het is de eerste verdedigingslinie tegen ongeautoriseerd gebruik.

03

GDPR-proof synchroniseren: ***do's & don'ts***

Het synchroniseren van data via API's brengt onmiskenbare voordelen met zich mee, maar het kan ook risico's creëren als het niet correct wordt uitgevoerd. ***Door te voldoen aan GDPR-richtlijnen kun je deze risico's minimaliseren.*** In dit hoofdstuk delen we de ***belangrijkste do's en don'ts*** voor veilige, efficiënte en compliant API-synchronisatie.

Do

01

Versleutel data

Data die via een API wordt verstuurd, moet altijd versleuteld zijn. Dit geldt voor ***zowel gegevens die worden verzonden ("in transit") als opgeslagen data ("in rust").*** Zonder encryptie kunnen kwaadwillenden API-verzoeken onderscheppen en gevoelige klantinformatie uitlezen.

Do 01

Versleutel data

- ***Gebruik altijd HTTPS*** voor API-endpoints; vermijd onbeveiligde verbindingen (zoals HTTP).
- Zorg dat ***certificaten up-to-date*** zijn om de betrouwbaarheid van je verbindingen te waarborgen.
- ***Gebruik sterke encryptiealgoritmes,*** zoals AES-256, om gegevens veilig te versleutelen.

Do

02

Log & monitor
je api calls

Door het gebruik van logging kun je vastleggen ***welke data wordt gedeeld,*** wie toegang heeft gehad, en ***welke acties*** er zijn uitgevoerd. Dit is niet alleen nuttig voor troubleshooting, maar ook essentieel voor GDPR-compliance.

Do 03

Log & monitor je api calls

- Zorg dat ***logs geen gevoelige gegevens*** bevatten. Bijvoorbeeld: sla alleen het type data op (zoals "e-mailadres verstuurd") en niet de exacte inhoud.
- ***Controleer*** regelmatig op ***verdachte activiteiten,*** zoals ongebruikelijk hoge volumes van API-calls.

Do

03

Log & monitor
je api calls

Stuur ***alleen de gegevens die strikt noodzakelijk zijn*** voor de betreffende toepassing. Hoe minder data je deelt, hoe kleiner het risico op overtredingen of datalekken.

Do

03

Log & monitor
je api calls

Praktisch voorbeeld, als je een e-mailmarketingtool synchroniseert met je CRM, volstaat het om alleen e-mail adressen en opt-in-voorkeuren te delen. Gegevens zoals geboortedata of aankoopgeschiedenis zijn vaak niet nodig.

Do 04

Gebruik sterke ***authenticatie en autorisatie***

Beperk toegang tot je API's door middel van geavanceerde authenticatiemethoden. Volgende methoden worden het vaakst gebruikt.

Do 04

Volgende methoden worden het vaakst gebruikt voor authenticatie

API-key

Een ***unieke sleutel die toegang verleent tot de API.*** Deze wordt vaak gegenereerd voor specifieke gebruikers of applicaties.

OAuth 2.0

Een protocol dat vaak gebruikt wordt voor veilige toegang tot API's. Het maakt gebruik van ***tokens die tijdelijk en specifiek zijn*** voor een bepaalde sessie of handeling.

Basic Authentication

Dit is ***een eenvoudigere methode*** waarbij een ***gebruikersnaam en wachtwoord*** worden gebruikt. Hoewel minder geavanceerd, kan het met TLS nog steeds veilig zijn.

Do 04

Gebruik sterke ***authenticatie en autorisatie***

Enkele praktische tips

- Maak gebruik van ***rolgebaseerde toegang*** (RBAC) om verschillende niveaus van toegang te beheren.
- Gebruik ***tokens*** die verlopen (bijvoorbeeld OAuth-tokens), zodat toegang niet permanent is.
- Monitor het gebruik van ***authenticatiesleutels*** en vervang deze regelmatig om risico's te minimaliseren.

Do 05

Documenteer je dataprocessen

Maak een overzicht van welke gegevens via API's worden verzonden, naar welke partijen, en met welk doel. Dit helpt niet alleen om ***compliant te blijven,*** maar biedt ook transparantie voor klanten en toezichthouders.
Toepassing: Stel een Data Protection Impact Assessment (DPIA) op als je gevoelige data via API's verwerkt.

Don't 01

Gebruik geen ***onbeveiligde verbindingen***

API-verzoeken die via HTTP worden verzonden, zijn ***kwetsbaar voor onderschepping en manipulatie.*** Ondanks de eenvoud van een HTTP-configuratie is het absoluut noodzakelijk om HTTPS te gebruiken.
Waarom? ***Zonder encryptie*** kunnen wachtwoorden, API-keys, of persoonsgegevens ***gemakkelijk door derden worden onderschept.***

Don't 02

Hardcode geen API-keys of wachtwoorden

Het opnemen van API-keys of wachtwoorden in de codebase is een ***veelvoorkomende fout die je systeem kwetsbaar maakt voor aanvallen.*** Als kwaadwillenden toegang krijgen tot je code, hebben ze meteen toegang tot je API's.

Don't 02

Hardcode geen API-keys of wachtwoorden

- Sla API-keys op in ***een beveiligd secrets management-systeem,*** zoals AWS Secrets Manager, HashiCorp Vault, of Azure Key Vault.
- Zorg ervoor dat sleutels ***regelmatig worden vernieuwd*** en zorg voor een strikte toegangscontrole.

Don't 03

Verstuur geen ***onnodige gegevens***

Overmatige datadeling is ***een directe overtreding van GDPR-principes*** zoals dataminimalisatie en doelbinding. Dit verhoogt het risico op datalekken én boetes.

Don't 03

Verstuur geen ***onnodige gegevens***

Bijvoorbeeld, bij het synchroniseren van een e-commerce CRM met een externe tool worden volledige klantprofielen (inclusief telefoonnummers, adressen en aankoopgeschiedenis) gedeeld, terwijl alleen de naam en e-mail nodig zijn.

make it fly

API calls en GDPR

Don't 04

De compliance van ***derde partijen negeren***

Veel bedrijven gaan ervan uit dat externe tools en softwareleveranciers automatisch GDPR-compliant zijn. Dit is echter niet altijd het geval.

Don't 04

De compliance van ***derde partijen negeren***

Wat te doen?

- Controleer of leveranciers ***GDPR-conform werken,*** vooral als ze buiten de EU zijn gevestigd.
- Sluit een ***Data Processing Agreement (DPA)*** af waarin je duidelijke afspraken maakt over de verwerking en opslag van gegevens.

Don't 05

De lifecycle van data negeren

Nog een belangrijke om niet uit het oog te verliezen, is dat GDPR niet alleen draait om dataverzameling, maar ook om dataverwijdering. API's kunnen data blijven synchroniseren, zelfs als een gebruiker heeft gevraagd om verwijdering.

Don't 05

De lifecycle van data negeren

Oplossing, zorg dat je systemen up-to-date blijven met wijzigingen, zoals verwijderverzoeken of correcties, en synchroniseer deze wijzigingen via API-calls.

04 case study

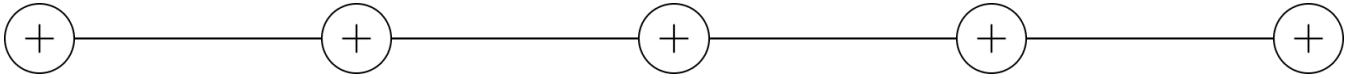
GDPR in *de praktijk*

make it fly

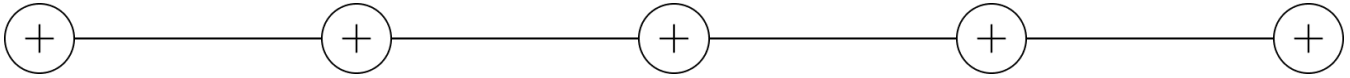
API calls en GDPR

case

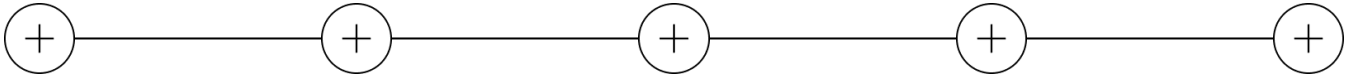
Een middelgroot e-commercebedrijf wilde zijn ***CRM-systeem (gehost in de EU) koppelen aan een e-mailmarketingtool (gehost in de VS).*** Het probleem? Het synchroniseren van klantdata moest GDPR-compliant zijn, terwijl de tool zich buiten de EU bevond.



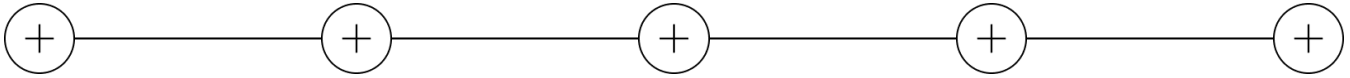
Het team bracht in kaart ***welke gegevens*** nodig waren voor de synchronisatie.



Alleen e-mailadressen en voorkeuren werden gedeeld, ***geen namen*** of aankoopgeschiedenis.



Gegevens werden verzonden via een ***versleutelde API*** met strikte ***toegangscontroles.***



Met de Amerikaanse toolaanbieder werden ***duidelijke afspraken*** gemaakt ***over dataopslag en verwerking.***

Het bedrijf deed het nodige om compliant te werk te gaan, en had ***een efficiënte synchronisatie*** tussen systemen. Het ***klantvertrouwen*** bleef intact, en de tool verbeterde de ***marketingprestaties.***

05

Tools & *checklist*

Praktische tools voor veilige api synchronisatie

Data Loss Prevention

(DLP-tools) Detecteer en voorkom ongewenste data-uitwisseling.

Postman

Test je API-calls en controleer welke data wordt verzonden.

API Gateways

(AWS API Gateway) Implementeer beveiliging op API-niveau, zoals throttling en authenticatie.

Ultieme checklist voor GDPR compliance

01

Heb je toestemming voor het verwerken van persoons-gegevens?

02

Is de data versleuteld tijdens de overdracht?

03

Gebruik je dataminimalisatie in je API-calls?

04

Zijn je derde partijen (softwareleveranciers) compliant?

05

Houd je logs bij van API-verzoeken en -antwoorden?

06

Heb je een Data Processing Agreement met relevante partijen?

GDPR-compliant en efficiënt werken, ***het kan!***

make it fly

API calls en GDPR

Je CRM synchroniseren via API's biedt ***grote voordelen,*** maar brengt ook verantwoordelijkheden en risico's met zich mee. Door te ***voldoen aan de GDPR-regelgeving*** kun je niet alleen juridische risico's vermijden, maar ook ***het vertrouwen van je klanten versterken.***

* *Disclaimer*

Deze whitepaper biedt algemene informatie en richt zich op praktische aspecten van het werken met API's en GDPR.
Voor sluitend juridisch advies bevelen we aan om een ***juridisch professional*** te raadplegen.

Hoe kunnen we ***jou helpen?***

Contacteer ons

make it fly®

Customer experience
gedreven ***IT groep***

Wij zijn ...

We bundelen de kracht van IT en creativiteit om jullie ***klantenservice***, ***digitale efficiëntie*** en ***communicatie*** te lanceren en te optimaliseren.

make it fly®

We ***transformeren*** complexe digitale ecosystemen naar ***intuïtieve*** en ***efficiënte oplossingen***

Daag ons maar uit, *we hebben niets liever*

#Durf te vragen

Bram Goffings
Chief technical officer
Bram.goffings@makeitfly.group

make it fly