Markteffect
Your data & insights partner

WHITEPAPER SECURITY

Markteffect

Informatiebeveiligingsbeleid en GDPR bij Markteffect: Uitgebreide FAQ voor Opdrachtgevers

Dit FAQ-document is een proactief hulpmiddel voor opdrachtgevers met vragen over ons informatiebeveiligingsbeleid en onze omgang met de GDPR (AVG). Als marktonderzoeksbureau verwerken wij dagelijks gevoelige gegevens van respondenten uit enquêtes en interviews, persoonsgegevens van panelleden en vertrouwelijke klantinformatie. Ons beleid is volledig afgestemd op het voorkomen van risico's zoals datalekken, reputatieschade en boetes.

De basis van ons beleid wordt gevormd door de ISO 27001:2022 norm voor ons Information Security Management System (ISMS), gecombineerd met de principes van de GDPR, zoals rechtmatigheid, doelbinding en gegevensminimalisatie. Dit document bevat de vragen die het meest gesteld worden aan ons over deze onderwerpen, voorzien van gedetailleerde en begrijpelijke antwoorden.

Markteffect

Certificeringen en naleving

Wat is de scope van de ISO 27001-certificering bij Markteffect?

De ISO 27001:2022-certificering omvat alle activiteiten binnen Markteffect, inclusief kwantitatief en kwalitatief marktonderzoek, paneelbeheer en data-analyse. Dit is vastgelegd in de Statement of Applicability (SoA). In de praktijk betekent dit dat alle verwerkingen van persoonsgegevens, zoals NAW-gegevens in enquêtes, onder ons ISMS vallen. Zo vermijden we risico's op non-compliance en zorgen we voor continue verbetering via audits.

De certificering is geldig tot december 2026 en wordt jaarlijks gecontroleerd. Bij wijzigingen, zoals de implementatie van een nieuwe survey-tool, voeren we een impactanalyse uit om de scope waar nodig aan te passen. Dit beschermt niet alleen onze eigen processen, maar geeft opdrachtgevers ook de zekerheid dat hun data veilig wordt behandeld, bijvoorbeeld door projectdata strikt te scheiden in de mappenstructuur.

Hoe zorgt Markteffect voor naleving van ISO 27001:2022?

Bij Markteffect hebben we een volledig geïmplementeerd Information Security Management System (ISMS) dat voldoet aan de eisen van ISO 27001:2022. Dit houdt in dat we risico's systematisch identificeren, beheersen en continu verbeteren via de PDCA-cyclus (Plan-Do-Check-Act). Dit omvat jaarlijkse interne en externe audits en risicoanalyses om te garanderen dat alle processen – van dataverzameling tot rapportage – veilig zijn. De directie is eindverantwoordelijk en behandelt de naleving in de jaarlijkse directiebeoordeling, waarin actiepunten uit audits worden opgevolgd.

Wat gebeurt er bij een externe audit van ISO 27001:2022?

Jaarlijks vindt een externe surveillance-audit plaats, waarin ons ISMS wordt getoetst op effectiviteit. Dit gebeurt door middel van interviews met medewerkers en controle van documenten zoals risicoanalyses. Eventuele bevindingen, zoals een onvolledige DPIA, worden als corrigerende acties geregistreerd in Jira en gerapporteerd in de directiebeoordeling. De auditresultaten delen we intern en op verzoek met opdrachtgevers om transparant te zijn, in lijn met het auditrecht onder de GDPR.

Wat is de rol van de directie in de naleving?

De directie is eindverantwoordelijk voor het ISMS. Dit betekent dat zij het beveiligingsbeleid goedkeuren, risico's beoordelen en middelen toewijzen, zoals budget voor trainingen. Ze nemen deel aan de jaarlijkse directiebeoordeling, waarin audits en incidenten worden besproken en verantwoordelijkheden worden toegewezen.

Moet Markteffect voldoen aan de NIS2-richtlijn?

Hoewel we niet direct verplicht zijn, integreren we de principes van NIS2 vrijwillig in ons ISMS om cyberrisico's effectief te beheren. Markteffect valt als middelgrote marktonderzoeksorganisatie niet direct onder de NIS2-richtlijn, omdat we niet worden aangemerkt als een 'essentiële' of 'belangrijke' entiteit binnen de 18 kritieke sectoren die de richtlijn definieert (zoals energie, zorg of digitale infrastructuur). De richtlijn is gericht op organisaties waarvan een verstoring door een cyberincident een significant maatschappelijk of economisch effect kan hebben.

Voldoet Markteffect aan de BIO-richtlijnen van de overheid?

De Baseline Informatiebeveiliging Overheid (BIO) is verplicht voor Nederlandse overheidsorganisaties. Voor een private onderneming als Markteffect is de BIO niet verplicht, tenzij dit contractueel wordt vereist door een overheidsopdrachtgever. Dankzij onze ISO 27001:2022-certificering, die de basis vormt voor de BIO, voldoen we al aan de kernprincipes.

NEN-EN-ISO/IEC 27001
GECERTIFICEERD
DOOR STICHTING
TOETSINGSBUREAU KCC

De link tussen GDPR en ISO 27001 bij Markteffect

De GDPR en ISO 27001:2022 vormen samen de basis voor ons informatiebeveiligingsbeleid. De GDPR is de wettelijke verplichting voor het verwerken van persoonsgegevens, terwijl ISO 27001 de internationaal erkende standaard biedt voor een systematisch ISMS dat helpt om aan deze eisen te voldoen. Binnen de context van marktonderzoek zorgt ISO 27001 voor een risicogebaseerde structuur die GDPR-principes, zoals doelbinding en gegevensminimalisatie, praktisch uitvoerbaar maakt.

Wat is de basis voor de verwerking van persoonsgegevens bij Markteffect?
Wij verwerken persoonsgegevens altijd op basis van een wettelijke grondslag uit de GDPR, meestal op basis van toestemming (voor deelname aan enquêtes) of gerechtvaardigd belang (voor panelbeheer). Hierbij passen we strikte dataminimalisatie toe: we verzamelen alleen gegevens die essentieel zijn voor het onderzoeksdoel. Voor verwerkingen met een hoog risico, zoals onderzoek naar gezondheid, voeren we standaard een Data Protection Impact Assessment (DPIA) uit.

Hoe anonimiseert Markteffect enquête-antwoorden?
Anonimisering is een cruciaal proces waarbij we persoonlijke identifiers (zoals IP-adressen en contactgegevens) direct na verzameling onomkeerbaar verwijderen. Dit zorgt ervoor dat de data niet meer herleidbaar is tot een specifiek individu, wat essentieel is voor de vertrouwelijkheid en het voorkomen van heridentificatie, met name bij open antwoorden in kwalitatief onderzoek.

Wat is een verwerkersovereenkomst en wanneer wordt deze gebruikt?
Een verwerkersovereenkomst (DPA) is een verplicht contract onder de GDPR tussen ons (de verwerker) en de opdrachtgever (de verwerkingsverantwoordelijke). Hierin leggen we exact vast hoe we persoonsgegevens verwerken, inclusief beveiligingsmaatregelen, de inzet van subverwerkers en de procedure bij incidenten. Bij elke contractaanvraag sturen we ons standaard DPA-sjabloon mee.

Welke rol speelt HeyData in het GDPR-beleid van Markteffect?
HeyData fungeert als externe partner en Data Protection Officer (DPO) en ondersteunt ons met juridische en compliance-kennis over privacy en databeveiliging. Zij helpen ons bij het opstellen en beoordelen van privacygerelateerde documenten, zoals privacyverklaringen en verwerkersovereenkomsten.

Beveiligingsmaatregelen

Welke technische en organisatorische maatregelen (TOMs) treffen jullie?
Onze beveiliging is gebaseerd op een gelaagde aanpak van technische en organisatorische maatregelen (TOMs), zoals vereist door de GDPR en ISO 27001.

Technische maatregelen

- Versleuteling van gegevens in rust
- Sterk wachtwoordbeleid en –beheer
- Implementatie van multi-factor authenticatie
- Gebruik van firewalls om het netwerk te beschermen
- Regelmatige patches en updates van systemen en software
- Implementatie van endpoint security op alle apparaten
- Beperking van toegang tot gevoelige gegevens op basis van rollen en rechten
- Monitoring van netwerkactiviteit en logboekregistratie
- Gebruik van geavanceerde malwarebescherming
- Implementatie van geografische beperkingen voor toegang tot gegevens
- Gebruik van geavanceerde netwerksegmentatie
- Implementatie van security information and event management (SIEM) systeem.
- Implementatie van geavanceerde e-mailbeveiligingsmaatregelen zoals DMARC, SPF en DKIM
- Gebruik van geautomatiseerde beveiligingscontroles en workflows
- Gebruik van geavanceerde endpoint detectie- en responsoplossingen (EDR)
- Implementatie van geavanceerde netwerkbeveiligingsprotocollen zoals IPsec
- Gebruik van geavanceerde dataclassificatie en labeling
- Implementatie van geavanceerde gegevensback-up- en hersteloplossingen
- Gebruik van geavanceerde beveiligingsprotocollen voor draadloze netwerken zoals WPA2
- Stringent beleid inzake logische toegangsbeveiliging
- Sterke SSL encryptie van websites (TLS 1.2 of hoger)

Beveiligingsmaatregelen

Hoe beveiligen jullie de fysieke en logische toegang?

Fysiek: Toegang tot onze kantoren is beperkt via persoonlijke tags en een intercomsysteem. Bezoekers worden altijd begeleid. Onze serverruimtes zijn voorzien van biometrische sloten en 24/7 monitoring.

Logisch: Toegang tot data is gebaseerd op het need-to-know-principe met rolgebaseerde toegangscontrole (RBAC). Medewerkers hebben alleen toegang tot de projectmappen die voor hen relevant zijn. Voor authenticatie is MFA verplicht.

Wat is jullie procedure bij een datalek of beveiligingsincident?

Bij een (vermoeden van een) datalek activeren we direct ons incident-response-proces. We informeren de opdrachtgever binnen 24 uur.

Organisatorische maatregelen

- Opstellen en implementeren van een informatiebeveiligingsbeleid
- Toewijzen van verantwoordelijkheden voor informatiebeveiliging aan specifieke personen of teams
- Opstellen en onderhouden van een register van verwerkingsactiviteiten
- Uitvoeren van data privacy impact assessments (DPIA's) voor nieuwe projecten of processen, indien noodzakelijk
- Opstellen van interne richtlijnen en procedures voor gegevensbeveiliging
- Implementeren van een bewustwordingsprogramma voor medewerkers over privacy en informatiebeveiliging
- Uitvoeren van regelmatige interne audits en controles op gegevensbeveiliging
- Implementeren van een systeem voor autorisatie en goedkeuring van toegang tot gegevens
- Opstellen van procedures voor het veilig verwijderen van gegevens na afloop van de bewaartermijn
- Implementeren van maatregelen voor het beheer van mobiele apparaten en externe werkomgevingen
- Periodiek evalueren en bijwerken van het informatiebeveiligingsbeleid en procedures
- Uitvoeren van regelmatige risicobeoordelingen voor gegevensbeveiliging
- Ontwikkelen van procedures voor het beheer van rechten en toegangscontroles
- Implementeren van een proces voor het periodiek herzien van gebruikersrechten en -toegang
- Opstellen van een beleid voor het veilig opslaan en archiveren van gegevens
- Documenteren van procedures voor het veilig delen van gegevens binnen en buiten de organisatie
- Ontwikkelen van een procedure voor het beoordelen en selecteren van externe dienstverleners op basis van gegevensbeveiligingscriteria
- Opstellen van procedures voor het beheer van toegangsrechten bij personeelswijzigingen
- Ontwikkelen van een beleid voor het veilig gebruik van externe opslagmedia en apparaten
- Implementeren van een proces voor het evalueren en selecteren van software en tools op basis van gegevensbeveiligingscriteria
- Opstellen van een beleid voor het veilig verwijderen en vernietigen van verouderde gegevensdragers
- Implementeren van maatregelen voor het beheer van gegevensoverdracht en -uitwisseling met externe partijen
- Ontwikkelen van een procedure voor het monitoren van wijzigingen in gegevensverwerkingssystemen

Leveranciers en subverwerkers

Hoe selecteren en beheren jullie leveranciers?
We classificeren leveranciers in vier niveaus, afhankelijk van hun impact op onze dienstverlening, en beoordelen hen jaarlijks op 16 criteria, waaronder ISO-certificering en de aanwezigheid van een DPA. We eisen dat data binnen de EER wordt opgeslagen en vragen vooraf toestemming voor de inzet van subverwerkers.

Welke subverwerkers gebruiken jullie?
Voor onze projecten kunnen we, afhankelijk van de aard van het onderzoek, gebruikmaken van subverwerkers. De data die opgeslagen wordt bij onze subverwerkers opgeslagen binnen de Europese Eeconomische Ruimte en zij werken conform de richtlijnen van de AVG. Daarnaast zijn met alle subverwerkers strenge afspraken gemaakt over de technische en organisatorische maatregelen die zij nemen om (persoons)gegevens vanuit Markteffect veilig te houden.

Nieuwe subverwerkers worden enkel toegevoegd na uitvoerige leveranciersbeoordeling en geen enkele subverwerker deelt data buiten de EER.

Risicobeheer en medewerkersbewustzijn

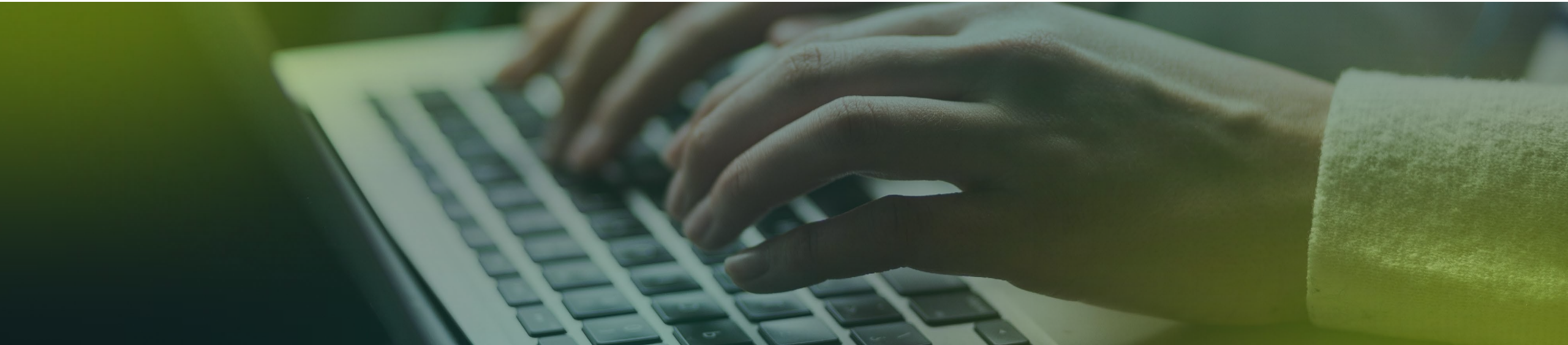
Hoe trainen jullie medewerkers op het gebied van beveiliging en GDPR?
Medewerkers volgen verplichte jaarlijkse trainingen via ons interne ME Academy-programma. Onderwerpen als dataklassificatie, het melden van incidenten en de GDPR-principes komen hierin uitgebreid aan bod. Alle medewerkers ondertekenen bovendien een geheimhoudingsverklaring (NDA) als onderdeel van hun arbeidsovereenkomst.

Hoe wisselen jullie data veilig uit met opdrachtgevers?
Data-uitwisseling gebeurt uitsluitend via beveiligde kanalen met end-to-end encryptie. We vermijden onbeveiligde methoden. Ruwe respondentdata wordt altijd geanonimiseerd voordat deze wordt gedeeld om heridentificatie te voorkomen.

Continuïteit en herstel

Hoe testen jullie het disaster recovery-plan?
We testen ons Disaster Recovery Plan (DRP) jaarlijks door middel van simulaties van scenario's zoals serveruitval. Hiermee valideren we onze herstelprocedures en minimaliseren we de impact van mogelijke calamiteiten.

Welke rol spelen back-ups in de continuïteit?
We maken dagelijks versleutelde back-ups van al onze kritieke data, die extern worden opgeslagen. De werking van deze back-ups wordt elk kwartaal getest door een herstelprocedure uit te voeren. Dit zorgt ervoor dat we dataverlies kunnen voorkomen en de dienstverlening snel kunnen hervatten na een incident.



Marktonderzoek en AI

Hoe gaat Markteffect om met het werken met Artificial Intelligence (AI)?
Bij Markteffect omarmen we technologische innovatie, waaronder Artificial Intelligence (AI), om de efficiëntie en kwaliteit van ons marktonderzoek te verbeteren. We zetten AI-tools echter altijd op een verantwoorde, veilige en ethische manier in, waarbij de bescherming van (persoons)gegevens en de vertrouwelijkheid van klantinformatie onze hoogste prioriteit heeft.

Onze aanpak is gebaseerd op drie kernprincipes:

- **Doelgerichte en ondersteunende inzet:** We gebruiken AI uitsluitend als hulpmiddel om onze onderzoekers te ondersteunen. Denk hierbij aan het analyseren van open antwoorden, het transcriberen van interviews of het formuleren van concept-vragenlijsten. AI neemt nooit de eindbeslissing; onze gespecialiseerde onderzoekers valideren, verfijnen en controleren altijd de output van een AI-model. Dit garandeert dat de methodologische kwaliteit en de betrouwbaarheid van de onderzoeksresultaten gewaarborgd blijven.

- **Strikte dataveiligheid en privacy (Zero Data for Training):** Wij hanteren een strikt beleid dat geen persoonsgegevens of vertrouwelijke klantinformatie wordt gebruikt voor het trainen van publieke AI-modellen. De AI-partners die we selecteren, zijn contractueel (via een verwerkersovereenkomst) verplicht om de door ons aangeleverde data volledig geïsoleerd te verwerken en niet te gebruiken voor andere doeleinden. Alle dataverwerking vindt plaats binnen beveiligde omgevingen in de EER, conform onze ISO 27001- en GDPR-standaarden.

- **Volledige integratie in ons ISMS:** De inzet van AI is geen losstaand proces, maar volledig geïntegreerd in ons Information Security Management System (ISMS). Elke AI-tool wordt behandeld als een subverwerker en doorloopt onze strenge selectie- en monitoringprocedure voor leveranciers. We voeren risicoanalyses uit en zorgen ervoor dat de inzet van AI voldoet aan alle relevante wet- en regelgeving, inclusief de principes van de GDPR.

Kortom, Markteffect zet AI in als een krachtig instrument om onze dienstverlening te verbeteren, maar altijd binnen de strikte kaders van ons ISO 27001-gecertificeerde beveiligingsbeleid en met een onwrikbare focus op de privacy van respondenten en de vertrouwelijkheid van onze opdrachtgevers.

Over Markteffect

Markteffect is een strategisch marktonderzoeksbureau dat als one-stop-shop dient voor haar opdrachtgevers. Vanuit onze kantoren in het centrum van Eindhoven en aan de Herengracht in Amsterdam werkt ons team van ruim 120 professionals dagelijks aan het achterhalen van de meest relevante data en inzichten voor een breed scala aan opdrachtgevers.

Data & Insights Bureau van het jaar 2025
Tijdens de uitreiking van Data & Insights Awards, georganiseerd door branchevereniging Data & insights Network, is Markteffect uitgeroepen tot hét Data & Insights bureau van het jaar 2025. Daarnaast werd Demian van Gils, Data Specialist bij Markteffect, bekroond met de titel 'Data Professional van het jaar'.

Wil je meer weten over onze andere onderzoeksmethoden, klik dan op één van de onderstaande buttons:

- Klanttevredenheidsonderzoek
- Medewerkertevredenheidsonderzoek
- Doelgroeponderzoek
- Customer journey onderzoek
- Sponser effectmeting
- Campagne pre-test

Markteffect

Bekijk voor meer informatie onze website
www.markteffect.nl

Markteffect