

# Privacy Policy Bureau Fris

Dit document beschrijft het totaal aan beveiligingsmaatregelen die door Bureau Fris zijn getroffen om de data van Bureau Fris en haar relaties zo optimaal mogelijk te beveiligen. Dit document bevat een combinatie van gedragsregels binnen Bureau Fris, een beknopte samenvatting van de technische beveiliging van de omgeving en de afspraken die zijn gemaakt met haar medewerkers.

## **Certificaten en keurmerken**

Bureau Fris beschikt over de volgende ISO-certificaten:

1. ISO 9001:2015
2. ISO 20252:2019

Daarnaast is Bureau Fris lid van de Marktonderzoek Associatie (MOA), een branchevereniging die de belangen van respondenten, gebruikers en aanbieders van marktonderzoek behartigt. Alleen organisaties die lid zijn van de MOA, en daarmee voldoen aan strenge kwaliteitseisen op het gebied van de omgang met persoonsgegevens, mogen het Fair Data keurmerk voeren en daarmee aan hun klanten en de consumenten zichtbaar maken dat data en privacy bij hun in vertrouwde handen is. Bureau Fris voldoet aan de strenge kwaliteitseisen van de MOA en beschikt over het Fair Data keurmerk.



## **Fysieke beveiliging**

Het kantoor van Bureau Fris is fysiek beveiligd door middel van sloten en alarmsystemen. Alle bezoekers dienen van tevoren te zijn aangemeld met voor- en achternaam. Externen zijn altijd onder begeleiding van een medewerker van Bureau Fris

Voor alle medewerkers van Bureau Fris geldt een "Clean Desk" policy zodat informatie niet door derden kan worden gelezen. Daarnaast wordt er twee keer per dag een security check uitgevoerd ('s ochtends en 's avonds) om eventuele datalekken te voorkomen of te detecteren. Dit wordt altijd gemeld bij de Data Protection Officer.

## **Data uitwisseling**

Binnen Bureau Fris geldt de regel dat alle data van klanten, bedrijven of personen niet wordt gedeeld met derden zonder uitdrukkelijke toestemming van de eigenaar van de gegevens. Dit geldt voor gesprekken, e-mail, schriftelijk en overige communicatie vormen.

## **Registratie van klanten**

Alle klant specifieke informatie wordt opgeslagen in een eigen maatwerk webapplicatie welke intern wordt gehost. Identificatie vindt plaats op basis van gebruikersnaam en wachtwoord. De verbinding vanuit de werkplek naar de server wordt encrypted door middel

van SSL (Secure Socket Layer) De applicatie is alleen toegankelijk voor degene die geautoriseerd zijn om met de applicatie te werken. Werknemers wijzigen hun wachtwoorden 2 keer per jaar.

### **Server beveiliging**

Hackers worden steeds slimmer en ransomware kan zich soms dagen in een systeem verstoppen voor het zich uit. Daar hebben wij onze back-up-strategie op aangepast. We bewaren back-ups op meerdere locaties en elke back-up wordt dagelijks gescand en gecontroleerd op ransomware. Bij de inrichting van de hele ICT-omgeving van Fris, hebben we gebruik gemaakt van een slimme rechtenstructuur. Zo kunnen mensen alleen bij die data die ze daadwerkelijk nodig hebben om hun werk te doen. Projecten waar ze niet aan bijdragen, daar hebben ze ook geen toegang toe.

### **Werkplekbeveiliging**

De werkplekken worden op een aantal manieren beveiligd:

- Er wordt geen data op de lokale werkstations bewaard
- De werkplekken worden beveiligd met een antivirus/malware/ anti-spyware pakket beveiligd
- Gebruikers mogen niet zonder toestemming van de directie, data dragers zoals dvd's, cd's, externe harddisk of usb sticks aan hun computer koppelen.
- Alle werkplekken worden regelmatig gecontroleerd op security patches en updates.
- Gebruikersrechten worden afgeschermd door middel van policies, waardoor zij alleen toegang tot de data hebben waarvoor zij zijn geautoriseerd door de Directie en Security Officers.
- Gebruikers zijn verplicht hun systeem te "locken" indien zij hun werkplek verlaten

### **Recruitment en persoonlijke data**

I.v.m. de AVG (Algemene Verordening Gegevensbescherming), welke van kracht is vanaf 1 mei 2018, communiceren wij alleen voornamen van onze respondenten. Tevens is het Bureau Fris niet toegestaan om e-mailadressen, woonadressen en telefoonnummers, IBAN-gegevens of andere herleidbare persoonsgegevens te delen met derden zonder toestemming van de respondenten. Wij gaan zeer zorgvuldig om met de persoonsgegevens van onze respondenten. Bijzondere persoonsgegevens, zoals iemands godsdienst, levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens, en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag, worden alleen verwerkt met nadrukkelijke toestemming van onze respondenten. Indien een klant herleidbare persoonsgegevens wenst te ontvangen t.b.v. het onderzoek, zullen hier administratiekosten voor worden berekend (vanaf 25,00 p.p.).

Indien het een telefonisch interview of een online onderzoek betreft, dan zitten de administratiekosten in de wervingskosten inbegrepen. Indien een opdrachtgever wel persoonsgegevens van de respondenten ontvangt, moet de opdrachtgever hiervoor een NDA of Verwerkersovereenkomst tekenen.

Het is niet toegestaan respondenten, geworven door Bureau Fris, voor/tijdens of na het onderzoek te benaderen voor uw eigen bestand, voor het bestand van derden of een andere reden anders dan het marktonderzoek. Contact gaat altijd via Bureau Fris. Als de opdrachtgever (u of uw klant) hier misbruik van maakt zijn wij genooddacht juridische stappen te nemen i.v.m. datalekken. Dit is opgenomen in de Verwerkersovereenkomst van Bureau Fris

Indien Bureau Fris een klantenlijst/bellijst ontvangt van haar klant, moet hiervoor een passende verwerkersovereenkomst worden getekend. Hierin wordt opgenomen welke informatie Bureau Fris

ontvangt en op welke manier Bureau Fris omgaat met de ontvangen data en het doel van verwerken. Bij het bellen uit klantenlijsten kunnen wij alleen bestanden inzien met daarin de gevraagde informatie (criteria). Indien er meer informatie in staat dan nodig, kunnen wij het bestand niet gebruiken in verband met de ISO 20252. Wij zullen de bestanden direct terugsturen en vernietigen uit onze mailserver. Bureau Fris koppelt geen gespecificeerde informatie terug over het klantenbestand. Dit houdt in dat Bureau Fris niet terugkoppelt wie er niet wilt deelnemen of wiens telefoonnummer niet klopt. Bureau Fris kan enkel een terugkoppeling geven in de vorm van een turflijst. Deze lijst bestaat uit geïnteresseerd, niet geïnteresseerd, foutief nummer en voicemail ingesproken. Bureau Fris mag niet doorgeven welke respondenten van de lijst niet mee willen doen i.v.m. anonimiteit. Bureau Fris raadt haar klanten aan om de bestanden te versleutelen en het wachtwoord door te bellen. Indien dit niet gedaan wordt, versleuteld Bureau Fris het bestand op haar eigen server. Bij het bellen van klantenlijsten zullen wij altijd de uiteindelijke opdrachtgever vermelden. M.a.w. versluiert uitnodigen van klantenlijsten is i.v.m. de AVG (Algemene Verordening Gegevensbescherming) niet mogelijk. Wij bewaren de klantenlijst uiterlijk 6 maanden en geven na 4 maanden een notificatie dat de lijsten worden verwijderd. Indien gewenst, wordt de lijst eerder na schriftelijk opdracht van de klant, verwijderd.

### **Facility**

Bureau Fris heeft een nieuwe en vooral veiligere manier om opnames te delen! Dertien jaar geleden begonnen wij met het opnemen op en uitdelen van VHS-banden. Vervolgens hebben wij lange tijd gewerkt met DVD's, terwijl wij de laatste jaren USB-sticks hebben meegegeven aan onze klanten. De techniek blijft zich echter hard ontwikkelen, wensen van de klanten veranderen en strengere eisen door GDPR zorgen ervoor dat wij overgaan op een nieuw systeem!

Bureau Fris heeft nu zijn eigen cloud waar klanten hun opnames van kunnen downloaden. Na afloop van het onderzoek zal een link verstuurd worden en een wachtwoord worden meegegeven aan de klant. Op deze manier kunnen klanten op een moment wanneer hen dit uitkomt en vanaf meerdere locaties de opnames downloaden. Hiermee is het delen van de opnames van onze onderzoeken een stuk simpeler, efficiënter en veiliger!

De download link zal een week lang actief zijn. Vervolgens zullen wij de back-up van de opnames nog een week langer intern bewaren alvorens wij deze vernietigen.

Zijn hier vragen over laat dit dan weten per mail, [facility@bureaufris.nl](mailto:facility@bureaufris.nl).

Voor aanvullende informatie over de Data Security van Bureau Fris, kunt u een e-mail sturen naar [Imane@bureaufris.nl](mailto:Imane@bureaufris.nl).