BUREAU FRIS B.V.
Baarsjesweg 224
1058 AA Amsterdam
+31 (0) 20 - 530 50 00
bureaufris.nl
recruitment@bureaufris.nl

Privacy Policy Bureau Fris

This document describes the total security measures taken by Bureau Fris to protect the data of Bureau Fris and its relations as optimally as possible. This document contains a combination of rules of conduct within Bureau Fris, a brief summary of the technical security of the environment and the agreements made with its employees.

Certificates and quality marks
Bureau Fris has the following ISO certificates:

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

Bureau Fris is also a member of the Market Research Association (MOA), a trade association that represents the interests of respondents, users and providers of market research. Only organizations that are members of the MOA, and thus meet strict quality requirements in regards to the handling of personal data, are allowed to carry the Fair Data quality mark and thus show their customers and consumers that data and privacy are in safe hands. Bureau Fris meets the strict quality requirements of the MOA and has the Fair Data quality mark.

Physical Security
The office of Bureau Fris is physically secured by means of locks and alarm systems. All visitors must be registered in advance with first and last name. External parties are always supervised by an employee of Bureau Fris

A “Clean Desk” policy applies to all Bureau Fris employees, so that information cannot be read by third parties. In addition, a security check is performed twice a day (in the morning and in the evening) to prevent or detect any data leaks. This is always reported to the Data Protection Officer.

Data exchange
Within Bureau Fris, the rule applies that all data of customers, companies or persons is not shared with third parties without the explicit permission of the owner of the data. This applies to conversations, e-mail, written and other forms of communication.

Customer registration
All customer-specific information is stored in its own custom web application which is hosted internally. Identification takes place on the basis of username and password.

The connection from the workplace to the server is encrypted by means of SSL (Secure Socket Layer). The application is only accessible to those who are authorized to work with the application. Employees change their passwords twice a year.

Server security
Hackers are getting smarter and ransomware can sometimes hide in a system for days before it shows itself. We have adapted our backup strategy to this. We keep backups in multiple locations and every backup is scanned and checked for ransomware on a daily basis. We made use of a smart rights structure when designing the entire ICT environment of Fris. This way people can only access the data they actually need to do their job. They don't have access to projects they don't contribute to.

Workplace Security
The workplaces are secured in a number of ways:
• No data is stored on the local workstations
• The workplaces are secured with an antivirus/malware/anti-spyware suite
• Users are not allowed to connect data carriers such as DVDs, CDs, external hard disk or USB sticks to their computer without permission from the management.
• All workplaces are regularly checked for security patches and updates.
• User rights are protected by policies, so that they only have access to the data for which they are authorized by the Management and Security Officers.
• Users are required to “lock” their system if they leave their workplace

Recruitment and personal data
In line with the GDPR (General Data Protection Regulation), which is effective from May 1, 2018, we only communicate the first names of our respondents. Bureau Fris will not share e-mail addresses, residential addresses and telephone numbers, IBAN data or other traceable personal data with third parties without the consent of the respondents. We handle the personal data of our respondents very carefully. Special personal data, such as a person's religion, belief, race, political opinion, health, sexual life, as well as personal data regarding membership of a trade union, criminal personal data, and personal data about unlawful or disruptive behavior in connection with a ban imposed as a result of that behaviour, are only processed with the explicit permission of our respondents. If a customer wishes to receive traceable personal data for the purpose of the research, administration costs will be charged for this.

If it concerns a telephone interview or an online survey, the administration costs are included in the recruitment budget. If a client does receive personal data from the respondents, the client must sign an NDA or Processor Agreement.

It is not permitted to approach respondents, recruited by Bureau Fris, before/during or after the research for your own panel, for the panel of third parties or for any other reason than the research project. Contact is always via Bureau Fris. If the client (you or your customer) abuses this, we are forced to take legal action to prevent data leaks. This is included in the Data Processing Agreement of Bureau Fris

If Bureau Fris receives a client list/call list from its customer, a suitable processing agreement must be signed for this.This includes what information Bureau Fris receives and how Bureau Fris handles the received data and the purpose of processing. When calling from client lists, we are only allowed to receive files containing the requested information (criteria). If it contains more information than necessary, we cannot use the file due to ISO 20252 regulations. We will immediately return the files and destroy them from our mail server. Bureau Fris does not provide any specified information about the client list. This means that Bureau Fris does not provide feedback on who does not want to participate or whose telephone number is incorrect. Bureau Fris can only provide feedback in the form of interested, not interested, wrong number and voicemail left. Bureau Fris is not allowed to indicate which respondents from the list do not want to participate.

Bureau Fris advises its customers to encrypt the files before sending them and contact us for the password. If this is not done, Bureau Fris encrypts the file on its own server. When calling client lists, we will always mention the end client. So, inviting clients from client lists is not possible without mentioning the end client due to the GDPR (General Data Protection Regulation). We keep the client list for 6 months at the latest and after 4 months we will notify you that the lists will be deleted. If desired, the list is deleted earlier after written confirmation from the client.

Facility

Bureau Fris has a new and above all, safer way to share recordings! Thirteen years ago we started recording and distributing VHS tapes. We then worked for a long time with DVDs, while in recent years we have been giving USB sticks to our customers. However, technology continues to develop rapidly, customer wishes are changing and stricter requirements due to GDPR mean that we are switching to a new system!

Bureau Fris now has its own cloud from which customers can download their recordings. After the project, a link will be sent and a password will be given to the customer. In this way, customers can download the recordings at a time that suits them and from multiple locations. This makes sharing the recordings of our projects a lot simpler, more efficient and safer!
The download link will be active for one week. We will then store the backup of the recordings internally for another week before we destroy them.

If you have any questions about this, please let us know by email to facility@bureaufris.nl.
For additional information about Bureau Fris' Data Security, please send an email to Imane@bureaufris.nl.