

WIFI: what are the practices for users and data controllers?

We are all used to using WIFI to connect to the Internet, at home, at work or in public places. However, for the user, this habitual gesture does not take on the same sensitivity depending on where the connection is made.

In addition, companies providing WIFI access have certain legal obligations, which vary depending on the purpose for which the access is provided. This factsheet aims to summarize the reflexes to adopt for all categories of data subjects affected by such processing.

What is WIFI?

WIFI is a trademark owned by the Wi-Fi Alliance consortium.

Any computer or smartphone manufacturer supplying a product compatible with one of the IEEE 802.11 (wireless network) standards must apply to the Wi-Fi Alliance (formerly WECA) for the right to use the name Wi-Fi and the corresponding logo.

The term « *WIFI* » is now widely known as a contraction of « *Wireless Fidelity* », but this explanation is somewhat erroneous...

The Wi-Fi Alliance consortium asked an advertising agency to come up with a more user-friendly name than « *IEEE 802.11b Direct Sequence Spread Spectrum* ».

The agency suggested several names, including « *Wi-Fi Alliance* », which sounded a bit like « *Hi-Fi* », a well-known brand in another field.

WIFI is based on the IEEE 802.11 standard. It is a wireless technology that enables all types of equipment (laptops, tablets, printers, mobile phones, games consoles, televisions, domestic appliances, industrial robots, etc.) to be connected to private professional networks and to the public Internet.

In the same way as your mobile phone, WIFI technology uses radio waves to transmit data across a network, so any equipment using WIFI has a wireless network adapter that will translate the data sent into a radio signal.

This same signal is then transmitted via an antenna (hotspot) to a decoder: the router. Once decoded, the data are sent to the Internet via a wired or optical connection from the box to the operator.

The term « *Hotspot* » is used to define an area where the WIFI connection is available.

If you use WIFI, what are the risks and what precautions should you take when away from home?

Many consumers are convinced that using a password to access WIFI guarantees the security of their information: this is not the case.

As the name suggests, public WIFI is « *open* », so you don't really need a code to connect. Sometimes an e-mail address is required to access it.

The main feature that attracts ill-intentioned people is that public WIFIs are not encrypted, but there are other risks, even if there is no ill intent on the part of the person providing the WIFI, such as:

- **collecting too much information** about you : for example, the CNIL has noted that data relating to the content of correspondence exchanged or information consulted (URLs) are often stored even though the service providers are not authorized to do so;
- **excessive retention of information** about you: the CNIL has noted that most service providers retain data from connection logs without defining a retention period. Traffic data must be kept for 1 year from the day it is recorded;
- **direct monitoring of Internet traffic.**

Therefore:

- when connecting to a free WIFI, make sure you are not connected to any of your applications beforehand;
- do not visit pages (websites) that require a login and password. Only visit authenticated pages (HTTPS). Think carefully before clicking on a link;
- turn off the WIFI « *application* », if it is not being used, and in particular the automatic reconnection: otherwise, if you connect to a malicious access point, your equipment could well remember this and automatically reconnect to it when the access point is within range again;
- keep your terminal up to date at all times;
- some WIFI networks are completely fictitious and exist solely to retrieve data. So stay vigilant. Don't hesitate to check the legitimacy of a network.

Generally speaking:

- avoid using a public WIFI to send/receive personal data, especially if you are not familiar with it;
- avoid entrusting too much personal data in exchange for free WIFI access;
- prefer to use your internet operator's 4G/5G network. If you have no choice, always visit HTTPS sites;
- opt for a VPN subscription that provides end-to-end encryption to ensure the confidentiality of the data you send and receive.

You are a company and you provide the public with WIFI Internet access:

- **You are concerned by the provisions of Law no. 1.430 on the preservation of national security (article 10) and its implementing Ministerial Order, as well as by articles 389-11-2 and 398-11-5 of the Penal Code**

Article 389-11-2 of the Monegasque Penal Code states that « *Operations aimed at deleting or anonymizing certain categories of technical data may be deferred for **a maximum period of one year** for the purposes of:*

1°) the implementation of the provisions of Law no. 1.430 of July 13, 2016 on various measures relating to the preservation of national security (...) »

Article 1 2° of the Ministerial Order implementing Article 10 of the aforementioned Law, for its part, stipulates that « *operators and service providers responsible for the operation of telecommunications and electronic communications networks and services (...) persons who offer access to electronic communications services to the online public, including free of charge (...) »* are qualified in particular, i.e. data controllers offering WIFI free of charge, or not, for their customers or visitors.

In this respect, they must therefore collect, « *excluding the contents of correspondence exchanged (...)- For the persons referred to in article 1 2°*

- 1° the connection identifier;*
- 2° the identifier assigned by these persons to the subscriber;*
- 3° the identifier of the terminal used for the connection when they have access to it;*
- 4° the start and end dates and times of the connection;*
- 5° the characteristics of the subscriber's line.*

- For the persons referred to in point 3 and point 2, when they collect them for their own purposes:

- 1° the connection identifier when the account is created;*
- 2° first and last name or company name;*
- 3° associated postal addresses;*
- 4° pseudonyms used;*
- 5° associated e-mail or account addresses;*
- 6° telephone numbers;*
- 7° the password and details of how to check or change it, in their last updated version;*
- 8° type of payment used;*
- 9° payment reference;*
- 10° the amount;*
- 11° date and time of transaction.*

May also be collected from all the persons referred to in Article 1, technical data relating to:

- 1° the location of terminal equipment;*
- 2° the access of terminal equipment to networks or online public communication services;*
- 3° the routing of electronic communications via the networks;*
- 4° the identification and authentication of a user, a connection, a network or an online public communication service;*
- 5° the characteristics of terminal equipment and their software configuration data ».*

Please note that article 389-11-5 of the Monegasque Penal Code specifies that «*The data kept and processed under the conditions defined in articles 389-11-2 to 389-11-4 relate exclusively to the identification of persons benefiting from or using the services provided by operators and service providers, to the technical characteristics of the communications provided by the latter and to the location of terminal equipment. **Under no circumstances may they relate to the content of correspondence exchanged or information consulted, in any form whatsoever, in the context of these communications. These data are stored and processed in accordance with the provisions of Law no. 1.165 of December 23, 1993 on the protection of personal data, as amended.***

Operators and service providers shall take all measures to prevent such data being used for purposes other than those provided for in this article.

Failure by operators or service providers responsible for the operation of telecommunications and electronic communications networks and services, or by one of their agents, to carry out operations to erase or render anonymous traffic data, where such operations are required by law, shall be punishable by one year's imprisonment and the fine provided for in point 3 of article 26.

Failure by operators and service providers responsible for operating telecommunications and electronic communications networks and services, or by one of their agents, to keep technical data under the conditions in which such keeping is required by law, shall be punishable by one year's imprisonment and the fine provided for in point 3 of article 26 ».

- **In view of the personal data you collect, you are a data controller under Law no. 1.565 of December 3, 2024**

The main features of this automated data processing system are as follows:

- the provision of Internet access via a WIFI terminal;
- informing the data subjects by means of a window/by accepting general conditions;
- the collection of identification details and connection logs of a data subject for a period of one year;
- restricting access to undesirable sites.

If you have at least 50 employees or if this processing is not occasional, you will need to list it in your register of processing activities.

And you should be aware of the security risks to your information system if your WIFI network is not watertight (secure).

In any event, collect data that is proportionate to the purpose for which WIFI is made available.

CAUTION: the provisions of Law no. 1.430 do not seem to apply if you are an employer who restricts WIFI to use by its employees. In this case, it is simply a specific method of connection by the company to the Internet network, which is covered by the « *Administrative management of employees* » processing operation. However, if you use a tool to monitor Internet use, the data subjects (the employees) must be informed of this monitoring and of their rights, whether the connection to the network is wired or by WIFI. An impact assessment may also be required.