EUROPEAN PARLIAMENT

TERMS AND CONDITIONS OF USE

Table of content

INTRODUCTION

This documents defines terms and conditions of use for the WIFI service proposed inside the European Parliament.

The WiFi service allows users with a compatible wireless device, to connect to the European Parliament wireless network.

The Service comprises of basic access functionalities to connect to the internet, the access to the internet and the rights defined for different user profiles.

1 - ACCESSING THE SERVICE

To access the Wifi service in the European Parliament, several categories of profiles are defined. In this document, the generic term to refer to these different profiles is the term "User".

The first group is made of:

- *Members of the European Parliament (MEP)*
- *Assistants,*

The second group:

- *Officials and staff of the European Parliament*
- *The staff of the political groups in EP,*
- *Contractors with " internal identification",*

The third group:

- *Contractors without "internal identification" such as freelance interpreters, visitors, media, and officials from other institutions.*

Depending of the rights defined by user groups, three access modes to the service are possible:

- access without authentication to european public websites,
- manual access using an access code,
- automatic access via the pre-installation of a certificate *(Group 1 & 2)*

Accessing the service is free of charge and possible at all times, except in cases of technical issue or maintenance period in the sites of Brussels or Strasbourg. Support is ensured during the normal opening hours of the European Parliament.

Terms and procedures for access for each group of users are defined in the annex at the description of service and accessible at the following link:

http://www.itsdnet.ep.parl.union.eu/sdesknet/cms/lang/en/Home/IT_Services/wifi

In case of problems the user should contact his /her IT support.[1]

Before accessing the service, the user needs to accept terms and conditions defined in this document and the technical identification should be validated on the systems by the appointed service.

[1] Refer to Section 2.5 in the description of service to find the corresponding service.

2 - COMMITMENTS AND RESPONSIBILITIES OF THE USER

- **Access Code for the service:**

Access Codes allow users to be identified and to connect to the Wifi service. They are personal and confidential.

If users in group 1 make the choice to benefit from the automatic authentication, they are responsible for the good management of the tool (the used device, the pre-installed certificate).

Users in group 3, receive their access code via a dedicated procedure.

Any access to the WiFi service in the EP, performed using the given access code of the user is made under his/ her sole responsibility.
The user agrees to keep secret access codes and to not disclose it in any manner or in any form to third parties.

By using his access codes, the user has personalised and exclusive access to the WiFi service.

- **Specific obligations related to the Internet:**

The use of the WiFi service of the European Parliament is subject to the respect of the principles below by the User.

The following provisions apply to all service users regardless of the type of profile.

– The User is solely responsible for any direct or indirect, material or immaterial, damage caused to third parties because of his/her personal use of the service.

– The User is solely responsible for the use of his/her access codes and terminal(s), whether personal or not, dedicated to the automatic or manual authentication.

– The User acknowledges having been informed that the integrity, authentication and confidentiality of information, files and data of any kind he wishes to exchange on the Internet can not be fully guaranteed on this network. The User must not transmit through the Internet, messages for which he would like to see kept private as guaranteed infallible.

– The User is solely responsible for the use of his credentials. Any use of data services, performed using the identification of the User is deemed to be made by the latter.

– The User undertakes not to use the service for illegal or prohibited purposes

As such, the User must comply with the legislation without the list below being exhaustive:

- The privacy of any person and compliance;

- Copyright and intellectual and industrial property, including multimedia creations, software, text, newspaper articles, photos, sounds, images of any kind, trademarks, patents, designs;
- The removal and / or reproduction of work or of any of these items and / or files and / or data without consent of the copyright owner constitutes an infringement
- The automatic processing of personal data, described by the applicable laws in force on the subject (see Article 6 of this document)
- Compliance with the rules of public order by issuing content information that would be likely to be posted on the Internet affecting the integrity or the sensitivity of the network users who could access messages, images or challenging texts;
- The secrecy of correspondence and the prohibition of interception of calls through telecommunications;

The User, through the use of the WiFi service, is also committed to respect the following rules:

- Not to defame, broadcast, harass, stalk, threaten anyone or violate the rights of others;
- Do not create a false identity;
- Do not attempt to gain unauthorized access to a service and / or a data
- Do not send junk or spam message;
- Do not send a message and / or e-mail containing offensive, defamatory, obscene, indecent, unlawful or infringing any rights, including human rights and the protection of minors;
- Do not transmit viruses, Trojan horses, time bomb or other harmful or destructive program for third parties and / or other Users;
- Do not attempt to gain unauthorized access to an automated data processing or to keep such access;
- Not to disrupt the services and / or content and / or data that are accessed;
- Do not send chain letters or offer sales also named 'snowball' or pyramid schemes;
- Do not send advertisements, promotional messages or other non-professional forms of unwanted solicitation;
- Do not deliberately create disturbance on the network by excessive usage of bandwidth (heavy downloads, continuous streaming, etc.).

- **Obligation in case of loss or theft of the terminal with a certificate dedicated to the automatic authentication.**

The User must immediately notify the Helpdesk to disable the certificate.

3 - COMMITMENT AND RESPONSIBILITIES OF THE EUROPEAN PARLIAMENT

- **Internet and Intranet Data security**

The European Parliament shall use all reasonable means at its disposal to ensure access and WiFi service reliability.

The European Parliament is not responsible for content accessible via the Internet (e.g. black lists) and damages that may arise from their use unless such damages have been caused intentionally by itself.

The User, if wishing increased protection and to restrict access to certain sites, servers or data, must ensure him or herself the acquisition of specific products from Internet security suppliers.

The responsibility of the European Parliament can not be engaged:

- In case of breach of its obligations by the User,
- In case of incompatibility or malfunction of a Wireless LAN network card of the mobile terminal with WiFi service proposed
- If unable to access via Internet a virtual private network of a company

- **Software Maintenance**

The European Parliament shall regularly update the content and software versions of the services offered. In this case, recall campaigns of equipment for the upgrading will be organized with a view to minimise the inconvenience to the user.

Software licenses paid by the European Parliament only cover the use of software corresponding to the user equipment. This right of use is not transferable to any other equipment.

- **Problem resolution**

The European Parliament is in charge of ensuring an appropriate performance of the WiFi network. For this purpose, it has the right to monitor the use of the WiFi network and its use by individual users and to take appropriate corrective measures and actions to solve potential problems.

The helpdesk will intervene in real time during business hours of the European Parliament with "best effort" to meet your constraints.

4 - SECURITY

The level of encoding of the radio channel may vary depending on the configuration profile of the user. For some of the defined profiles, the radio channel is not encrypted. The communications made through the WiFi service of the European Parliament have the same level of security as Internet communications standard.

To reinforce the security level, the user can set him/herself security software on his terminal as personal firewalls *(firewalls)* or VPN *(Virtual Private Network*).

To ensure confidentiality and integrity of data transmitted over the internal WiFi network, several encryption standards have been developed: WEP, WPA and WPA2, WPA2 offer better protection. All of these encryption protocols are limited to signals sent over the radio interface.

The User acknowledges having been informed that the integrity, authentication and confidentiality of information, files and data of any kind (credit card number, etc ....) he wishes to exchange on the Internet cannot be guaranteed on this network.

Total Protection against unauthorised access or eavesdropping can not be guaranteed. The European Parliament cannot be held responsible for such events.

It is expressly stated that the Internet is not a secure network. Under these conditions, it is up to the user to take all appropriate measures to protect his own data and / or software from a contamination by viruses circulating on the Internet or the intrusion in the system's terminal (laptop, Smartphone, etc.) for any purpose whatsoever, and to make backups before and after using the WiFi service of the European Parliament.

Users also acknowledge to be fully informed of the lack of reliability of the Internet, especially in terms of lack of security on the transmission of data and non-guaranteed performance for the volume and speed of data transmission.

Users recognise that they have been informed that the use of Bluetooth in parallel with the WiFi network is not recommended because it leads to collisions on the radio channel, which can adversely affect network performance. In addition, "ad-hoc WiFi" configurations are not allowed because they are disruptive to the performance of the European Parliament's network.

5 - SUSPENSION AND TERMINATION

The European Parliament reserves the right to suspend or terminate access to the WiFi service for violation of any of the provisions of these conditions of use and especially if:

- The European Parliament finds that the User fails to comply with the Terms and Conditions in force detailed in this document.

- The European Parliament is notified by rights holders that the User reproduces and/ or disseminates data protected by property rights.

- The European Parliament notes any piracy actions or attempted unauthorized use of the information circulating on the network being caused and originating from the user account.

6 - NO PERSONAL DATA AND PERSONAL INFORMATION

- **Protection of personal data**

The European Parliament deals with personal data pursuant to Regulation (EC) No 45/2001 of the European Parliament and the Council of 18 December 2000 on the processing of personal data.

This regulation aims to protect the freedom and fundamental rights of individuals with regard to the processing of personal data concerning them. The Regulation aims to facilitate the free flow of information within a framework guaranteeing the rights of people and their legitimate expectation of respect for privacy.

In this context, the European Parliament undertakes to respect the internal regulation of the European Parliament, described in the Personal Data Protection Guide accessible via the link: *http://www.europarl.europa.eu/pdf/data_protection/guide_en.pdf*

Any service within the European Parliament, such as WIFI service, that uses information identifying individuals is affected by these provisions. Any operation on this data (collection, storage, consultation, communication, organisation, etc...) must be communicated to the data protection officer through a notification. He lists the notification in a public registry.

To fulfil its obligations to its employees and citizens, the European Parliament may need to know personal information such as name and address or other, even more sensitive information.

- **Storage of data**

Pursuant to Directive 2006/24/EC of the European Parliament and the Council of 15 March 2006, the European Parliament is under an obligation to carry out the storage and retention of specific communication data.

This directive aims to harmonise Member States' provisions concerning the obligations of providers of electronic communications services available to the public or public communications networks in the conservation of certain data, which are generated or processed by them, to ensure the availability of this data for research, detection and prosecution of serious crime as defined by each Member State under its domestic law.

This Directive requires that the data be retained for emergency responses to security and terrorism. This data provides key evidence to solve cases of infringement and to ensure the rights.

The Directive requires the retention of data for a period ranging from six months to two years to, for example to:

- trace and identify the source of communications,
- trace and identify the destination of communications,
- identify the date, time and duration of communications,
- identify the type of communication,
- identify the machine used to communicate,
- identify the position of mobile communication equipment.