



UCOPIA COMMUNICATIONS:

The response to the legal obligations imposed upon organisations which provide access to the internet to members of the public in france and in the member states of the european union.



SOMMAIRE

1 | Background

2 | Focus on the legal framework in France, what you must know about the anti-terrorism act & other legal provisions in 5 points

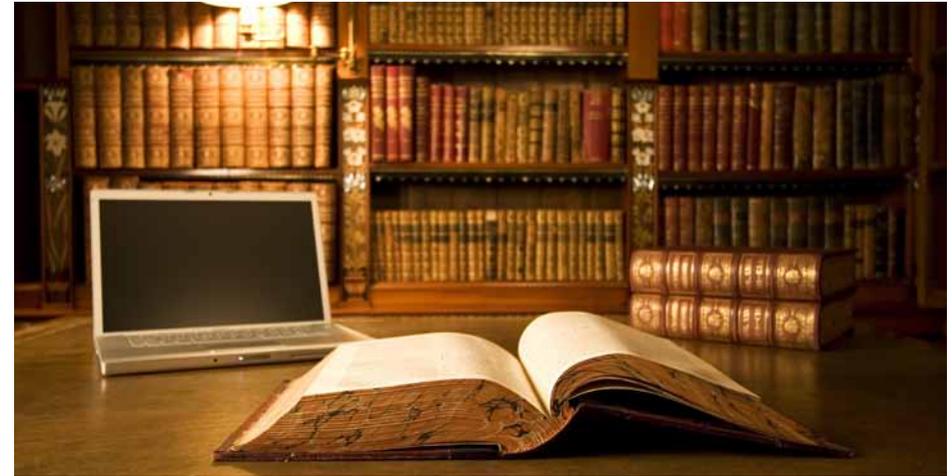
3 | Transposition of directive 2006/24/EC and periods of data retention imposed by the Member States of the European Union

4 | A suitable response: Our solution

5 | Our main media-intensive deployments in 2011

6 | About UCOPIA Communications

1 | BACKGROUND



Offering an access to the Internet to members of the public is no trivial matter.

Since France's law no. 2006-604 dated 23 January 2006 concerning measures to combat terrorism, cafés, hotels, cybercafés, restaurants, airports and anyone who offers to members of the public a connection enabling communication online via an access to the network, even free of charge, are legally bound to retain a number of traffic-related data.

This paper is designed to inform these persons who, being unaware of the obligations by which they are bound, often offer their clients a connection enabling communication via the Internet without having taken care to implement beforehand a system that would enable them to transmit to whomsoever it may concern the information that they were however legally bound to retain.

Because any failure to comply with these various obligations is liable to incur criminal punishment, it would seem useful to set them down here.

European Directive 2006/24/EC dated 15 March 2006 compels all of the Member States of the European Union to adopt a law obliging providers of electronic communication services that are accessible to members of the public and public communication networks to keep the data concerning the resulting communications for a period of time comprised between 6 and 24 months.

This paper therefore sets out information about the national legal systems which transpose this directive and what periods of retention they impose.

Sadry Porlon, an attorney and member of the bar in Paris. *Mr. Porlon is a doctor of law and also teaches at a business school, specialising in media and communication law as well as e-commerce and multimedia law.*

2 | ZOOM

Focus on the legal framework in France, what you must know about the anti-terrorism act & other legal provisions in 5 points

	The anti-terrorism act & other legal provisions	HADOPI law
An operator of electronic communication services must retain...	<ul style="list-style-type: none"> Information providing a means of identifying the user Data concerning the hardware and terminals used Data concerning the technical characteristics as well as the date, the time and the duration of each communication Data concerning the complementary services requested or used and their providers Data providing a means of identifying the recipients of the communication <p>(France's decree no. 2006-358 dated 24 March 2006, article R. 10-13 CPCE)</p>	
An operator of electronic communication services need not retain...	<p><i>"the content of the correspondence exchanged or information viewed, whatever the form thereof, in the course of these communications"</i></p> <p>(Article L. 34-I-V CPCE)</p>	
The punishments in case of non-compliance with the obligation to retain the data are...	<p>Up to one year in prison and a fine of 75,000 euros for natural persons and a fine of 375,000 euros in the case of legal persons.</p> <p>(Article L. 39-3 CPCE)</p>	
The period of retention of the data is...	<p>One year in the case of data concerning the traffic for purposes of detection, investigation and prosecution of offences.</p> <p>(France's decree of 24 March 2006 provides for variable periods of retention depending on the goals).</p>	

	<p>The data retained by the operator of electronic communication services can only be transmitted to duly empowered persons including:</p> <ul style="list-style-type: none"> the police officer during an on-the-spot investigation the District Attorney or the police officer authorised by the public prosecutor, during a preliminary investigation the investigating magistrate or the police officer instructed by the latter to take action as part of the investigation the individually empowered agents of the police forces specialising in the prevention of acts of terrorism <p>(Articles 60-1, 77-1-1 and 99-3 of France's code de procédure pénale [rules governing criminal procedures and evidence] as well as article L. 34-1-1 CPCE)</p> <p>Article L. 39-4 CPCE provides that: <i>"whomsoever shall, without any valid reason, refuse to provide the information or documents or impede the progress of the investigation shall be punished by three months' imprisonment and a fine of 30,000 euros or either one of these two punishments only"</i>.</p>	<p>The commission for the protection of the rights protected by the HADOPI law can ask an operator of electronic communication services to provide the following information:</p> <ul style="list-style-type: none"> the family name, first names; the postal address and electronic addresses; the telephone numbers; the address of the telephone facility of the subscriber. <p>(article 2 of France's decree no. 2010-236 dated 5 March 2010)</p> <p><i>"Any violation of the provisions of article R. 331-37 is punishable by the imposition of the fine scheduled for category 5 (highest) misdemeanours (i.e. 1,500 euros)"</i> This refers, in the case of an operator of electronic communication services, to any failure to disclose the personal data and the information mentioned in section 2 of the appendix of decree no. 2010-236 dated 5 March 2010 which is claimed from it.</p> <p>(Article R. 331-38 of France's decree no. 2010-872 dated 26 July 2010)</p>
The data to be provided to the persons empowered to receive it on pain of criminal punishments are...		

4 | TRANSPOSITION OF DIRECTIVE 2006/24/EC AND PERIODS OF DATA RETENTION IMPOSED BY THE MEMBER STATES OF THE EUROPEAN UNION

Study research : January 2012

Although France, via its decree no. 2006-358 dated 24 March 2006 concerning the retention of electronic communication records which followed on from France's law no. 2006-64 dated 23 January 2006 concerning anti-terrorist measures, did not need to transpose the Directive due to the fact that its internal law was already compliant, the 26 other European Union countries had to do so.

Directive 2006/24/EC of the European Parliament and of the European Council dated 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC defines the rules and the procedures of retention of personal data as well as registers of telephone calls that providers of electronic communication services that are accessible to members of the public and public communication networks must comply with.

This directive requires the retention of data concerning the traffic generated by the use of the electronic communication services during a period ranging from six months to two years¹.

It provides that the maximum period of retention of this data can be extended by a Member State if it "*faces specific circumstances which justify an extension, for a limited period*" and provided that this extension is notified to the Commission, which can, within six months following the notification, approve or reject the extension. Whereas the maximum duration can be extended, there is no legal provision to provide for a shortening of the period of retention to under six months.

The retention obligation applies to the data concerning the traffic itself and to the location data of both legal entities and natural persons, as well as to related data that is necessary to identify the subscriber or the registered user. It does not apply

to the content of the electronic communications, such as to the information viewed using an electronic communication network.

In accordance with article 5 of the directive, the categories of data to be retained are:

- a) data necessary to trace and identify the source of a communication
- b) data necessary to identify the destination of a communication
- c) data necessary to identify the date, time and duration of a communication
- d) data necessary to identify the type of communication
- e) data necessary to identify users' communication equipment or what purports to be their equipment
- f) data necessary to identify the location of mobile communication equipment

This directive was to be transposed mandatorily by 15 September 2007 by the Member States of the European Union.

The following table indicates the periods of retention of the data imposed by the countries of the European Union which, like France, had an obligation to transpose the Directive.

It mentions the countries in which the directive has not yet been transposed, but also the cases where court rulings have declared the laws passed by the national parliaments² transposing the directive as unconstitutional.

We should point out that there are also laws on the retention of the data in a number of countries which are not part of the European Union but which are members of the European Economic Area (EEA), including Iceland, Liechtenstein and Norway³.



¹ L'Article 6 of the directive provides that "Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication"

² Romania, the Czech Republic and Germany.

³ The Icelandic law is law no. 81/2003 on telecommunications as subsequently modified in April 2005. In Liechtenstein, the law is the 2006 law on telecommunications. In Norway, a law was passed on 5 April 2011.

Country	Laws which transpose the directive	Periods of retention of the data stipulated by the national laws	Comments
Germany	<p>The law revising the means of surveillance of the telecommunications sector and introducing other investigative measures as well as implementing Directive 2006/24/EC</p> <p>Publication date: 31/12/2007 Date on which the law came into force: 01/01/2008</p>	<p>12 months as of the date of the communication.</p> <p>Pending the introduction of a new law transposing Directive 2006/24/EC which might set a different duration</p>	<p>In a ruling delivered on 2 March 2010, the German Federal Constitutional Court declared that certain provisions of the German law which transposes the Directive were unconstitutional</p> <p>On 27 October 2011, the Commission formally urged Germany to adopt, within two months, measures designed to ensure full compliance with the rules of the EU concerning the retention of data</p>
Austria	<p>The 2003 federal law amending the law on telecommunications.</p> <p>Publication date: 18/05/2011 Date on which the law came into force: 19/05/2011</p>	6 months as of the date of the communication	
Belgium	<p>The law of 21 March 1991 introducing reforms to certain state corporations</p> <p>The Royal decree of 9 January 2003 implementing articles 46-II, § 2, par. 1, 88-II, § 2, pars 1 and 3, and 90-IV, § 2, par 3 of Belgium's criminal investigation code as well as article 109-III, E, § 2 of Belgium's law of 21 March 1991 introducing reforms to certain state corporations</p>	<p>12 to 36 months in the case of telephony services accessible to members of the public</p> <p>There still hasn't been any transposition for internet services</p>	<p>Belgium thus still awaits a law which might transpose Directive 2006/24/EC outright.</p> <p>A white paper on the retention of data filed on 27 August 2009 provides for a period of retention of 24 months.</p> <p>Certain players which have been polled have recommended curtailing the period of retention of data to 12 months</p>

Bulgaria	<p>Electronic Communications Act</p> <p>Publication date: 02/03/2010</p> <p>Date on which the law came into force: 10/05/2010</p> <p>Regulation # 40 dated 7 January 2008 on the categories of data and the procedure under which they would be retained and disclosed by companies providing publicly available electronic communication networks and/or services for the needs of national security and crime investigation</p> <p>Publication date: 29/01/2008</p> <p>Date on which the law came into force: 01/02/2008</p>	12 months as of the date of the communication. The data to which access is provided may be retained for six more months on request	<p>A challenge against the retention of data was filed before the supreme administrative court of Bulgaria (ruling no. 13627 of 11 December 2008)</p> <p>This led to a revision of the transposition law</p>
Cyprus	<p>The law on the retention of telecommunications data for the prevention of serious crimes.</p> <p>Publication date 31/12/2007 Date on which the law came into force: 31/12/2007</p>	6 months as of the date of the communication	<p>Several challenges against the retention of data have been brought before the Cypriot Constitutional Court (cases nos. 65/2009, 78/2009 and 15/2010-22/2010 on 1 February 2011). The Court ruled that the rulings of the courts that had been handed down by virtue of the transposition law were unconstitutional</p> <p>The transposition law nevertheless remains valid</p>

Denmark	<p>The first, second and third orders on providers of electronic communication networks and electronic communication services concerning the recording and storage of traffic-related information</p> <p>Publication date: 13/10/2006</p> <p>Date on which the law came into force: 15/09/2007</p>	12 months as of the date of the communication	
Spain	<p>Law no. 25/2007 on the retention of data on electronic communications and public communication networks</p> <p>Publication date: 19/10/2007</p> <p>Date on which the law came into force: 08/11/2007</p>	12 months as of the date of the communication	A competent authority can, after consulting the operators of electronic telecommunications services, curtail this period of retention to 6 months or conversely increase it to 24 months for some data or categories of data
Estonia	<p>The law on electronic communications and public health</p> <p>Publication date and date on which the law came into force: 07/12/2007</p>	12 months as of the date of the communication	
Finland	<p>The law on the obligation to identify and store data / the law on the privacy of electronic communications</p> <p>Date on which the law came into force: 05/06/2008</p>	12 months as of the date of the communication	Finland does not impose upon small operators the obligation to retain data on the grounds that the costs that this would imply both for the provider and for the State would exceed the benefits for the forces of law and order and the criminal justice system

Greece	<p>The law on the retention of data generated or processed in partnership with the public communication networks, the use of surveillance systems, audio or video reception or recording in the public places and related provisions</p> <p>Publication date: 21/02/2011</p>	12 months as of the date of the communication	
Hungary	<p>The 2003 law on electronic communications</p> <p>Publication date: 13/12/2003</p> <p>The 2007 law amending the law on electronic communications</p>	6 months for unsuccessful telephone calls and 12 months for all other data	A challenge was brought on 2 June 2008 by the Hungarian civil liberties union before the Hungarian Constitutional Court. It is currently pending
Italy	<p>The law implementing Directive 2006/24/EC on the retention of the data generated or processed as part of the provision of electronic communication services or public communication networks and amending Directive 2002/58/CE</p> <p>Publication date: 18/06/2008</p>	12 months as of the date of the communication	
Ireland	<p>Communications (Retention of Data) Act 2011</p> <p>Publication date: 28/01/2011</p>	<p>24 months for land-line and mobile telephony data</p> <p>12 months for data concerning access to the Internet, e-mail via the Internet and telephony over the Internet</p>	

Latvia	<p>The amendments to the law on electronic communications of 17/11/2004</p> <p>Publication date: 24/05/2007</p> <p>Date on which the law came into force: 07/06/2007</p> <p>The procedures compelling operators of electronic communication services to gather and to retain statistical information about the data and to deliver it on request to the investigating authorities before a trial, to the emergency services, to the national security authorities and to the public prosecutor pursuant to court orders</p> <p>Publication date: 07/12/2007</p> <p>Date on which the law came into force: 08/12/2007</p>	18 months as of the date of the communication	
Lithuania	<p>Lithuania's law on electronic communications</p> <p>Publication date: 29/11/2008</p> <p>Date on which the law came into force: 15/03/2009</p>	6 months as of the date of the communication	
Malta	<p>The 2008 amended law on data protection (LN. 198)</p> <p>Publication date 29/08/2008</p> <p>The law on the regulation of electronic communications (LN. 198) (CAP 399)</p> <p>Publication date: 29/08/2008</p>	<p>12 months for any data concerning fixed, mobile and Internet telephony</p> <p>6 months for any data concerning access to the Internet and to e-mail via the Internet</p>	

The Netherlands	<p>The law of 18 July 2009 amending the law on telecommunications and economic crimes in connection with the implementation of Directive 2006/24/EC of the European Parliament and the Council of the European Union on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (law on the retention of the data from telecommunications)</p>	12 months as of the date of the communication	
Poland	<p>The Regulation of the Minister of Infrastructure of 28 December 2009 on a detailed specification of data and types of operators of public telecommunications networks or providers of publicly available telecommunications services obliged for its retention and Storage.</p> <p>The law of 24 April 2009 amending the law on telecommunications of 16 July 2004</p> <p>The decree of 22 March 2010 on the procedure for transmitting and sharing data in case of bankruptcy of an operator of a public telecommunications network or of a provider of telecommunications services accessible to members of the public</p>	12 months as of the date of the communication	
Portugal	<p>The transposition into national law of Directive 2006/24/EC of the European Parliament and of the European Council dated 15 March on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks</p> <p>Publication date: 17/07/2008</p>	12 months as of the date of the communication	

Czech Republic	<p>Law no. 247/2008 Coll. amending law no. 127/2005 Coll. on electronic communications and amending certain related laws</p> <p>Publication date: 04/07/2008</p>	<p>Between 6 and 12 months as of the date of the communication.</p> <p>Declared unconstitutional, it must now be transposed anew</p>	<p>A ruling of the Czech Constitutional Court on 22 March 2011 declared that law no.127/2005 and decree no. 485/2005 were unconstitutional. The Czech Republic is currently examining ways of proceedings with a new transposition of the Directive.</p>
	<p>Decree no. 485/2005 Coll. on the measurement of traffic and periods of retention of location data and its transmission to the bodies that are empowered to use them</p> <p>Publication date: 15/12/2005</p>		
Romania	<p>The law on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks amending law no. 506/2004 on the processing of personal data and privacy in the electronic communications sector.</p> <p>(law no. 298/2008)</p> <p>Publication date: 21/11/2008</p>	<p>6 months as of the date of the communication</p>	<p>On 8 October 2009, the Romanian Constitutional Court held that law no. 298/2008 transposing the Directive was unconstitutional.</p> <p>On 27 October 2011, the European Commission formally called upon Romania to adopt, within two months, measures designed to ensure full compliance with the rules of the EU concerning the retention of data</p>
United Kingdom	<p>The Data Retention (EC Directive) Regulations 2007</p> <p>Date on which the regulations came into force: 01/10/2007</p> <p>The Data Retention (EC Directive) Regulations 2009</p> <p>Date on which the regulations came into force: 06/04/2009</p>	<p>12 months as of the date of the communication</p>	<p>The United Kingdom does not impose upon small operators the obligation to retain data on the grounds that the costs that this would imply both for the provider and for the State would exceed the benefits for the forces of law and order and the criminal justice system</p>

Slovakia	<p>Law no. 654/2007 modifying and complementing law no. 610/2003 on electronic communications</p>	<p>12 months in the case of data relating to land-line and mobile telephony, 6 months for data concerning access to the Internet, e-mail via the Internet and telephony over the Internet</p>	
Slovenia	<p>The rules governing the method of transmission of the traffic data held by mobile telephony services and fixed electronic communications networks</p> <p>Publication date: 14/12/2009</p> <p>Date on which the law came into force: 13/01/2010</p> <p>The law amending the law on electronic communications</p> <p>Publication date: 12/12/2006</p>	<p>8 months in the case of data relating to the Internet.</p> <p>14 months in the case of telephony data</p>	
Sweden	<p>The Directive has not been transposed</p>	<p>12 months as of the date of the communication</p>	<p>Sweden was declared guilty of failing to comply with its EU obligation by the ECJ (C-185/09).</p> <p>In April 2011, the Commission brought a second appeal against Sweden before the Court for failing to abide by the ruling handed down in case C-185/09.</p> <p>Sweden runs the risk of incurring a fine in accordance with article 260 of the treaty on the operation of the European Union following the decision of its Parliament to defer by a year the passing of the transposition law.</p>

CONCLUSION

We have just seen what the Member States have decided concerning the duration of the obligation to retain the data relating to traffic and the location data that they were under an obligation to impose upon the operators of electronic communications services operating on their territory.

Even though some of the Member States have not yet transposed the Directive, or have witnessed their internal courts censor the law which was passed to transpose it, the provisions concerning the retention of data were always designed to assist the criminal justice systems and the forces of law and order of the European Union.

The Directive indeed provides that the data must be kept for purposes of investigation, detection and prosecution of serious offences.

An operator of electronic communications services which intends to provide access to

the Internet to members of the public in one of the 27 Member States of the European Union and specifically in those which, at present, have transposed Directive 2006/24/EC, must therefore ensure that it has the requisite technical facilities enabling the gathering of the data concerning the traffic and the location data of Internet users which precisely meets the recommendations of the law which transposes the Directive into internal law while keeping in mind that this data may only be disclosed to a restricted number of authorities which are empowered to secure delivery thereof.



For more informations :
<http://eur-lex.europa.eu>

4 | A SUITABLE RESPONSE: OUR SOLUTION

The UCOPIA solution meets the requirements of entities wishing to deploy a secure Internet connection (open-access Wi-Fi, guest connection) in order to comply with the 2006 anti-terrorism act.

These solutions, which are designed in particular for:

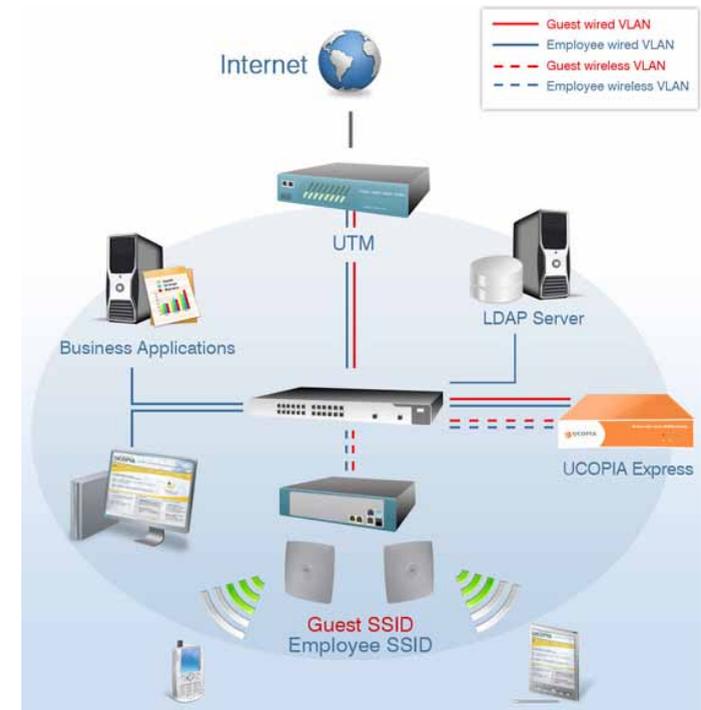
- companies,
- hotels,
- educational establishments,
- hospitals,
- or authorities,

enable users to connect securely to the network and to use the business applications, Internet or telephony facilities in a simple and secure manner.

The technical performance, the ease of installation, the stringent compliance of our captive portal with the regulations make it the leading product in its field.

The UCOPIA product range consists of two ranges: **Express range and the Advance range.**

The **UCOPIA Express range** consists of a hardware box that is ready for use and is perfectly suited to the requirements of hotels, clinics, secondary education establishments and SMEs in general. UCOPIA Express features most of the functions of UCOPIA in terms of security and support for roving users in an approach which focuses on simplicity of implementation and administration.



The **UCOPIA Advance** range consists of a hardware box featuring all of the UCOPIA functionality, aimed at medium or large size corporate projects, campuses and authorities. UCOPIA Advance meets the requirements of multiple-site environments and integrates within the company's LAN. UCOPIA Advance can be operated in redundant mode and also operates in load distribution mode.

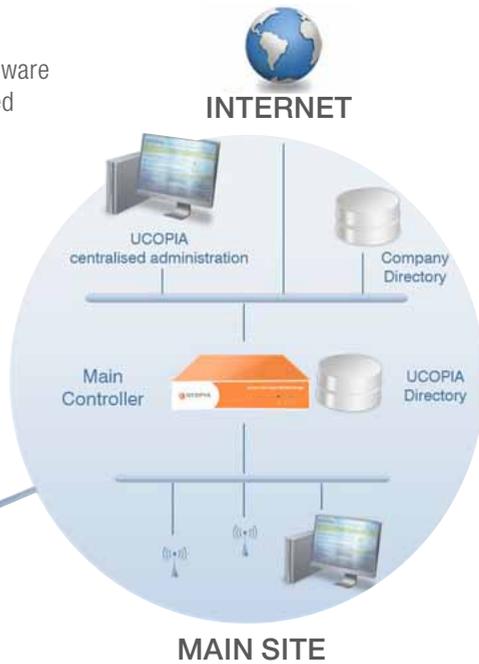
Our **two solutions** are designed to be positioned between a wire-based access network (ethernet, dslam, CPL) or wireless access network (Wi-Fi) and the LAN of the organisation.

All the streams from or to the user transit via the hardware unit so as to **guarantee security, simplify the coupling** with the LAN, **facilitate the administration** and **enhance the convenience for users**.

Depending on the model chosen, our solutions can manage between **5 and more than 1000 concurrent users** and are easy to install in the network infrastructure.

UCOPIA mobile applications

- Simplified authentication
 - One-time only input of identifiers upon first connection, with automatic playback thereafter
 - Automatic recognition of a UCOPIA controller
- Rapid creation of user accounts
 - Delegation
 - Choice of the profile and of the period of validity
 - Choice of the contact from the directory of the telephone
 - Sending of identifiers by SMS or e-mail.
- Available in French and in English
- Downloadable free of charge since from the various application "stores"



UCOPIA is the only product which combines:

- **An analysis of the streams** (Who does What, When and How)
- **A database** used to store connection logs, view and analyse data
- **A local disk** and automatic online storage for archiving the logs

THE MAIN ADVANTAGES OF THE SOLUTION ARE

- A comprehensive and scalable product range (supporting more than 1000 concurrent connections)
- A security system combining authentication, access control via profile and traceability of connections: UCOPIA is the only product certified by ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information)
- A captive portal that is fully customisable
- Ease of installation and administration
- Accurate management of performance indicators
- Ease of use (multiple home portals)
- Zero configuration access (no need for technical support)
- A return on investment in less than 6 months
- 90% lower operating costs



5 | OUR MAIN MEDIA DEPLOYMENTS IN 2011

Crous de Lyon uses UCOPIA solutions enabling the management of connections by students and by the personnel on both wire-based and Wifi infrastructure (more than 200 access points).

The UCOPIA solution is deployed in 29 university student residences and in the 15 restaurants of CROUS.



CROUS DE LYON



INTERCONTINENTAL.

UCOPIA has fitted out 5 hotels of this prestigious hotel chain. A bespoke captive portal was implemented in order to welcome clients in keeping with the hotel's charter. A "Click and surf" concept was developed to handle tablet computers, Smartphones and personal computers. UCOPIA was integrated into the business software application (PMS), the automatic management of clients is optimised thanks to registration via SMS, e-mail, and self-registration.

LILLE GRAND PALAIS

Lille Grand Palais deployed Wi-Fi transmitters to provide an optimal service during trade fairs, conferences and shows. This service is combined with UCOPIA routers and servers.

The infrastructure can handle up to 2000 concurrent connections.



MÉDIPOLE SANTÉ

INTERCONTINENTAL HÔTELS



The Internet at the service of patients: tablet computers, Smartphones and other personal computers have become indispensable tools of our day-to-day lives. Medipole

Santé has implemented the UCOPIA solution on its Wifi infrastructure in order to comply with the law and offer in complete security Internet access to its patients and their visitors. The provision of this Internet access has improved the quality of their patients' stay, enabling them to communicate with their relatives.

L'ORÉAL

L'Oréal uses UCOPIA solutions enabling it to offer Internet access to roving employees and visitors over a Wi-Fi infrastructure.



7 | ABOUT UCOPIA COMMUNICATIONS



UCOPIA has installed systems for more than:

1500 hotels



450 healthcare establishments



1000 SMEs and large corporations



800 schools



750 public bodies

UCOPIA Communications, which was founded in 2002, is the leader on the market for access control systems for visitors & roving employees.

The UCOPIA solution is certified by l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information) which is France's national regulator of information systems security.



UCOPIA Communications sells its products through a European network of several hundred integrators, experts in the fields of networking, IP convergence and security, but also specialising in specific sectors of activity (hotels, education, SMEs, etc.).

Thanks to the expertise of this network of partners, UCOPIA can advise and assist its clients in their projects, whatever their size and sector of activity.

UCOPIA COMMUNICATIONS IN BRIEF:

- More than **6,000 clients** in all sectors of activity
- A network of more than **150 partners** in Europe
- More than **100 million connections** in 2011 using our solutions
- **50% annual growth** over the past six years
- Based in **Paris**, with offices in **Munich and Milan**

Please see below for a small selection of our clients who have chosen to trust us with their security.

HOTELS



HEALTH



EDUCATION



COMPAGNIES



LOCAL AUTHORITIES





www.ucopia.com

UCOPIA Communications
201, Avenue Pierre Brossolette 92120 - MONTRouGE - FRANCE
Tél. : + 33 (0) 1 40 92 73 90 - Fax : + 33 (0) 1 40 92 73 99
Email : contactus@ucopia.com