

		Implementat ion directive 2006/24/CE	National law reference	Onsite Inspections/Questio nnaire	Type of services (Y/N)		
Num	Countries				Mobile	Fixed	Internet
1	Belgium	No		Questionnaire	Yes	Yes	Yes
2	Bulgaria	Yes	Law on Electronic Communications (LEC)- Art. 250a-f,251 and 251a	Yes. Inspections of the mobile operators were conducted and the questionnaire on the first joint investigation action was sent to them.	Yes	Yes	Yes
3	Cyprus	Yes		Both	Yes	Yes	Yes

		Implementat ion directive 2006/24/CE	National law reference	Onsite Inspections/Questio nnaire	Type of services (Y/N)		
Num	Countries				Mobile	Fixed	Internet
4	Czech Republic	Yes	Act No. 127/2005 Coll, as amended	both	Yes	Yes	Yes
5	Denmark	Yes	Danish Ministerial Order 988/2006	Questionnaire	Yes	Yes	Yes
6	Estonia	Yes	Estonian Electronic Communications Act	Questionnaire	Yes	Yes	Yes

		Implementat ion directive 2006/24/CE	National law reference	Onsite Inspections/Questio nnaire	Type of services (Y/N)		
Num	Countries				Mobile	Fixed	Internet
7	Finland	Yes	Protection of Privacy in Electronic Communication 343/2008	Questionnaire	?	?	?
8	France	Yes	decree n° 358/2006	Onsite Inspections	Yes	Yes	Yes
9	Germany	Yes	Sections 113a and 113b of the Federal Telecommu- nications Act (TKG)	both	Yes	Yes	Yes

		Implementat ion directive 2006/24/CE	National law reference	Onsite Inspections/Questio nnaire	Type of services (Y/N)		
Num	Countries				Mobile	Fixed	Internet
10	Greece	No		both	Yes	Yes	Yes
11	Hungary	Yes	ACT C / 2003	Both	Yes	Yes	Yes
12	Ireland	No		Both	Yes (no SMS)	Yes	Yes

		Implementat ion directive 2006/24/CE	National law reference	Onsite Inspections/Questio nnaire	Type of services (Y/N)		
Num	Countries				Mobile	Fixed	Internet
13	Italy	Yes	Decree no. 109/2008	both	Yes	Yes	Yes
14	Latvia	Yes	Electronic Communications Law	both	Yes	Yes	Yes

		Implementat ion directive 2006/24/CE	National law reference	Onsite Inspections/Questio nnaire	Type of services (Y/N)		
Num	Countries				Mobile	Fixed	Internet
15	Liechtenstein	No		Questionnaire	Yes	Yes	Yes
16	Lithuania	Yes	Law on electronic communications n° IX 2135	Both	Yes	Yes	Yes.Pursuant to Article 15(3) of the Directive 2006/24/EC Lithuania has declared that it will postpone the application thereof to the retention of communications data relating to internet access, internet telephony
17	Luxembourg	No		Both	Yes	Yes	Yes

		Implementat ion directive 2006/24/CE	National law reference	Onsite Inspections/Questio nnaire	Type of services (Y/N)		
Num	Countries				Mobile	Fixed	Internet
18	Malta	Yes	LN 198/2008 and LN 199/2008	Questionnaire	Yes	Yes	Yes
19	Netherlands	Telecommuni catio Data Retention Act July 7th 2009	31.145	both	Yes	Yes	Yes
20	Poland	No		both	Yes	Yes	Yes

		Implementat ion directive 2006/24/CE	National law reference	Onsite Inspections/Questio nnaire	Type of services (Y/N)		
Num	Countries				Mobile	Fixed	Internet
21	Romania	Yes	Act no. 298/2008 (Constitutional Court has declared unconstitutional)	Both	Yes	Yes	?
22	Slovak republic	Yes	No. 610/2003 Coll. on electronic communications	Questionnaire	Yes	Yes	Yes
23	Slovenia	Yes	Electronic Communications Act ZEKom-UPB1(Off. Gaz. of RS, no. 86/04, 129/06 and 110/09)	both	Yes	Yes	Yes

		Implementat ion directive 2006/24/CE	National law reference	Onsite Inspections/Questio nnaire	Type of services (Y/N)		
Num	Countries				Mobile	Fixed	Internet
24	Spain	Yes	Act 25/2007	both	Yes	Yes	Yes
25	UK	Yes	Data Retention Regulations 2009	Questionnaire	Yes	Yes	Yes

		Traffic data		
Num	Countries	Mobile	Fixed	Internet
1	Belgium	Load ID, Record Type, served IMSEI, served IMEI, cell identity ci served MSISDN, served Ip-address, client Ip-address	start date, start time, call duration	login, logout, duration, in/out, IP no content data collected
2	Bulgaria	number of the caller, ID data of subscriber or user; dialed number, number to which the call was transmited; date and hour of the beginning and the ending of the call; type of the used public telephone service; IMSI, of the caller and the calling, IMEI, date and hour of service activating and location	IP addresses, telephone number of user and ID data, caller and called telephone number	User ID, number of any message entering the public telephone network, number of the receiver of Internet telephone call, date and hour of entering or exiting the Internet (logs), dynamic and static IP address for Internet access, ID of user and subscriber, date and hour of entering or exiting e-mail, caller telephone number, DSL and other connection end point.
3	Cyprus	CDR (part A-part B) callID, duration, time , cellID, subscriber identity, IMSI, IMEI	CDR (part A-part B) callID, duration, time	IP address e-mail headres

		Traffic data		
Num	Countries	Mobile	Fixed	Internet
4	Czech Republic	telephone number of the calling party and the called party, date and time of commencement of traffic, duration of traffic, the IMEI number, the StartBTS station number and, as appropriate, the StopBTS station number, destination	telephone number of the calling party and the called party or the identifier of the telephone card for use in a public pay phone, date and time of commencement of traffic, duration of traffic	IP address, PORT NUMBER user account, identifier of the message on the mail server, date and time of commencement of traffic, sender's electronic mail addresses, recipients' electronic mail addresses, identifier of the electronic mail protocol, quantity of transferred data
5	Denmark	no details	no details	no details
6	Estonia	<ul style="list-style-type: none"> • the number making the call (A-number); • the number receiving the call (B-number); • date and time when the call started; • duration of the call and / or date and time when the call ended IMSI, IMEI, cell-ID	<ul style="list-style-type: none"> • the number making the call (A-number); • the number receiving the call (B-number); • date and time when the call started; • duration of the call and / or date and time when the call ended 	the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, allocated by the Internet access service provider to a communication, and the user ID of client

		Traffic data		
Num	Countries	Mobile	Fixed	Internet
7	Finland	no details	no details	no details
8	France	day, hour, incoming and outgoing phone numbers, IMSI, type call		IP addresses (no content, no email)
9	Germany	<ul style="list-style-type: none"> • A, B and (if applicable) C number • date and time when the call started and ended • IMSI, IMEI, cell-ID • all above mentioned applies to regular calls as well as SMS or MMS • if different services are available as part of the telephone service, data on the service used 	<ul style="list-style-type: none"> • A, B and (if applicable) C number • date and time when the call started and ended • if different services are available as part of the telephone service, data on the service used 	<p>email:</p> <ul style="list-style-type: none"> • identifier of electronic mailbox and IP of the sender and recipient • identifier and Internet Protocol address used to access electronic mailboxes • date and time of the log-in and log-off <p>internet access:</p> <ul style="list-style-type: none"> • IP assigned to the subscriber • unequivocal identifier of the end point of the originator used to access • date and time of the log-in and log-off

		Traffic data		
Num	Countries	Mobile	Fixed	Internet
10	Greece	calling and called number, date, time and duration of the call, IMSI and IMEI codes of calling and called number as well as the antenna (cell)	CDR, identification of the caller and the recipient of the telephone call, the duration of the call, the cause of call termination and some data about the internal routing of the call	a timestamp, the username, the assigned IP address SMTP, POP3 and IMAP protocol logs the header of the email message
11	Hungary	dialing and the called numbers, discrete technological identifiers, user identifiers, the type of the electronic telecommunicational service, date, the time, when it started and ended, incidentally the transmitter calls, IMEI, IMSI, the network and cell-identifier, and the data necessary for geographical identification	calling and the called number, discrete technological identifiers, user identifiers, the type of the electronic telecommunicational service, date, the time, when it started and ended, incidentally the transmitter calls	sender and destination, address of origin and type, discrete technological identifiers, user identifier, the type of the electronic telecommunicational service, date, the time, when it started and ended (for emails too), IP adress, user identifier
12	Ireland	no details	no details	no details

		Traffic data		
Num	Countries	Mobile	Fixed	Internet
13	Italy	CDR (part A-part B) callID, duration, time , cellID, subscriber identity, IMSI, IMEI	CDR (part A-part B) callID, duration, time	a timestamp, the username, the assigned IP address the header of the email message (1 case)
14	Latvia	<ul style="list-style-type: none"> • the number making the call (A-number); • the number receiving the call (B-number); • date and time when the call started; • duration of the call and / or date and time when the call ended IMSI, IMEI, cell-ID	<ul style="list-style-type: none"> • the number making the call (A-number); • the number receiving the call (B-number); • date and time when the call started; • duration of the call and / or date and time when the call ended call transfer	One operator retained content (1 month)

		Traffic data		
Num	Countries	Mobile	Fixed	Internet
15	Liechtenstein	no details	no details	the records of the RADIUS server no data as to contents
16	Lithuania	- the number making the call (A number); - the number receiving the call (B number); - subscriber identity; - date and time when the call started; - duration of the call and /or date and time when the call ended VOIP, SMS, EMS (2 inspected companies providing mobile telephony services)	- the number making the call (A number); - the number receiving the call (B-number); subscriber identity; - date and time when the call started; - duration of the call and/or date and time when the call ended	IP address, e-mail logs (source, destination, date and time)
17	Luxembourg	CDR	CDR	CDR

		Traffic data		
Num	Countries	Mobile	Fixed	Internet
18	Malta	timestamp, location	timestamp	IP address Radius log e-mail logs (source, destination, date and time)
19	Netherlands	The categories of data that are to be retained under the Telecommunications Data Retention Act are the same categories of data that are listed in article 5 of the Data Retention Directive 2006/24/EC.	The categories of data that are to be retained under the Telecommunications Data Retention Act are the same categories of data that are listed in article 5 of the Data Retention Directive 2006/24/EC.	The categories of data that are to be retained under the Telecommunications Data Retention Act are the same categories of data that are listed in article 5 of the Data Retention Directive 2006/24/EC.
20	Poland	MSISDN (mobile telephone number), IMEI number (telephone serial number), IMSI (number connected with telephone serial card number), roaming number, data and time when a call starts and ends, LAC/CELL ID (location area code/cell identifier), user's contact details (name, surname, place of residence)	source of call (caller telephone number), data necessary to establish a recipient (recipient telephone number), data essential do establish date, time and duration of call, as well as data necessary to identify type of call (type of telephone service being used e.g. 'alarm clock', forwarding).	session start/end (date, time), IP number, login and parameters of access and service router which enable to identify TP subscribers CONTENT ON REQUEST BY PUBLIC AUTHORITY

		Traffic data		
Num	Countries	Mobile	Fixed	Internet
21	Romania	<ul style="list-style-type: none"> • the number making the call (A-number); • the number receiving the call (B-number); • date and time when the call started; • duration of the call and / or date and time when the call ended IMSI, IMEI, cell-ID	<ul style="list-style-type: none"> • the number making the call (A-number); • the number receiving the call (B-number); • date and time when the call started; • duration of the call and / or date and time when the call ended IMSI, IMEI, cell-ID	no details
22	Slovak republic	(for details see Annex4 of the Act No 610/2003 Coll.); CDR (part A-part B) callID, duration, time , cellID, subscriber identity, IMSI, IMEI	(for details see Annex4 of the Act No 610/2003 Coll.); CDR (part A-part B) callID, duration, time	(for details see Annex4 of the Act No 610/2003 Coll.);IP addresses (type of service data), IPDR, Internet telephony CDR
23	Slovenia	<ul style="list-style-type: none"> • the number making the call (A-number); • the number receiving the call (B-number); • date and time when the call started; • duration of the call and / or date and time when the call ended IMSI, IMEI, cell-ID	<ul style="list-style-type: none"> • the number making the call (A-number); • the number receiving the call (B-number); • date and time when the call started; • duration of the call and / or date and time when the call ended call transfer	e-mail: date and time of communication, message ID, sender e-mail, recipients' e-mail, status (e.g. sent) internet access: calling telephone number (dial-up), IP address, the digital subscriber line (DSL) or MAC address (end point), date and time of the log-in and log-off of the Internet access service, user ID, type of communication

		Traffic data		
Num	Countries	Mobile	Fixed	Internet
24	Spain	MSISDN, IMEI, IMSI the origin cell from which the call was initiated and the destination cell of the call -and those indicated in the Directive	CDR (part A-part B) callID, duration, time	IP address, email sender-destination timestamp
25	UK	Calling Telephone (Source of communication) Name & address of the subscriber or registered user of any such telephone Telephone No dialled including where appropriate the telephone number to which the call is forwarded or transferred (Destination of communication) Name & address of the subscriber or registered user of any such telephone. Date, time, start and end of call. The telephone service used International Mobile Subscriber Identity (IMSI) and the International Mobile Equipment Identity of the telephone from which the call was made	Calling Telephone No (Source of communication) Name & address of the subscriber or registered user of any such telephone Telephone No dialled including where appropriate the telephone number to which the call is forwarded or transferred (Destination of communication) Date, time, start and end of call. The telephone service used (type of communication)	iThe user ID allocated The user ID and telephone number allocated to the communication entering the public telephone network. The name and address of the subscriber or registered user to whom an IP address, user ID or telephone number was allocated at the time of the communication. In the case of Internet telephony, the user ID or telephone number of the intended recipient of the call. In the case of internet e-mail or internet telephony, the name and address of the subscriber or registered

		Retention period (months)			Communication channel towards LEAs
Num	Countries	Mobile	Fixed	Internet	
1	Belgium	it varies (12--> 24 months)			fax/ mail/ specific section
2	Bulgaria	12	12	12	The access to the data is performed after court decision and is exercised by the submission of motivated written request for inquiry by the competent authorities. The data can be provided to competent authority from other country if foreseen in international agreement, entered in force in the Republic of Bulgaria.
3	Cyprus	6	6	6	provided in person

		Retention period (months)			Communication channel towards LEAs
Num	Countries	Mobile	Fixed	Internet	
4	Czech Republic	6-->12	6-->12	6-->12	Mostly specific encrypted channels; in one company data were handed over to the appointed police agent
5	Denmark	12	12	12	data based on requests at the operator's address
6	Estonia	12	12	12	paper inside closed envelope, direct access, protocol HTTPS

		Retention period (months)			Communication channel towards LEAs
Num	Countries	Mobile	Fixed	Internet	
7	Finland	no details	no details	no details	PGP
8	France	12	12	12	fax/ encrypted mail
9	Germany	6	6	6	<ul style="list-style-type: none"> • FAX • PGP email • CD-ROM or DVD-ROM via snail mail

		Retention period (months)			Communication channel towards LEAs
Num	Countries	Mobile	Fixed	Internet	
10	Greece	retention periods vary drastically (2 years-->5 yeras)			sealed envelopes, registered mail, fax (in one case also encrypted mail)
11	Hungary	retention periods vary depending on internal orders in the investigated companies			Open and Classified requests are divided depending on national security screening. Online data requests of NSS and National Security Authority (NSA) are provided by a service provider - Lawful Data Providing System.
12	Ireland	36	36	6	encrypted e-mail

		Retention period (months)			Communication channel towards LEAs
Num	Countries	Mobile	Fixed	Internet	
13	Italy	24	24	12	certified email/FAX
14	Latvia	In most cases 18 Up to 36	In most cases 18 Up to 36	In most cases 18 Up to 36	in writing (by post) and electronically

		Retention period (months)			Communication channel towards LEAs
Num	Countries	Mobile	Fixed	Internet	
15	Liechtenstein	6	6	6	the data are handed over either personally or in encrypted form
16	Lithuania	6+6	6+6	6+6	Encrypted e-mail, hard copy, web interface secured by https protocol (the transmission channel is encrypted by SSL channel)
17	Luxembourg	6	6	6	In general, operators follow the instructions received from Law Enforcement Authorities without further analysis. Authorised staff provides the required information on paper, CD or USB stick directly to the requesting agent.

		Retention period (months)			Communication channel towards LEAs
Num	Countries	Mobile	Fixed	Internet	
18	Malta	12	12	6	e-mail, CD, hard copy format, soft copy through a single contact point
19	Netherlands	12	12	12 -> 6	There are existing protocols and procedures for handling information requests from the authorities. PGP is used when transmitting traffic data, and the encrypted traffic data is always sent to (previously known) named individuals.
20	Poland	it varies from provider to provider for each service (longest 10 years)			electr. mail and encryption/authent. with public key

		Retention period (months)			Communication channel towards LEAs
Num	Countries	Mobile	Fixed	Internet	
21	Romania	6->36	6->37	6->38	in electronic format, encrypted by courier by mail
22	Slovak republic	6 - Mobile services : Internet access , Internet e-mail, Internet telephony ; 12 - other types of mobile services	6 - Fixed neetwork services : Internet access , Internet e-mail, Internet telephony ; 12 - other types of fixed network services ;	6 - Internet access service , Internet e-mail, Internet telephony	Personal receipt by the authorised LEA Officer, Encrypted e-mail
23	Slovenia	14	14	8	paper or portable electronic media, by courier, secure e-mail

		Retention period (months)			Communication channel towards LEAs
Num	Countries	Mobile	Fixed	Internet	
24	Spain	6<12	6<12	6<12	certified email/encrypted mail/hand deliver
25	UK	12	12	10-->12	SSL preferred method, fax and email. Pre directive / existing methods of transferring traffic related data to specified authorities

		Logical security measures	Physical security measures
Num	Countries		
1	Belgium	<p>no encryption of traffic data</p> <p>access to data is strictly restricted (id/pw)</p> <p>risk assessment (50%)</p> <p>Security certification (50%)</p> <p>Appointed CISO</p> <p>penetration test</p> <p>access log management</p> <p>No logging of system admin</p>	<p>access control through cards</p> <p>systems against intruders</p> <p>Video Surveillance Closed Circuits</p> <p>alarm response centres</p> <p>Security guards</p> <p>UPS (50%)</p> <p>fire detection systems, flood protection (50%)</p>
2	Bulgaria	<p>Obligation for implementation of necessary technical and organizational measures, forbidden listening, recording, storing and other ways of intercepting or tracking of messages of other individuals. No retention of content data. Deletion of data after the set period.</p> <p>Only the authorised persons have access to the data that are necessary for their work</p> <p>There is access log management for traffic data</p> <p>No encryption</p>	<p>alarm system, physical control of an entrance</p> <p>video-surveillance, anti-incendiary measures</p> <p>premise with limited entrance, guard</p>
3	Cyprus	<p>risk assessment (50%)</p> <p>audit (50%)</p> <p>no security certification</p> <p>no CISO</p> <p>penetration test (no specific)</p> <p>access to data is strictly restricted (id/pw)</p> <p>access log management (50%) - no encryption (only in transmission)</p>	<p>Access control through cards</p> <p>Systems against intruders</p> <p>Video surveillance</p> <p>Security guards</p>

		Logical security measures	Physical security measures
Num	Countries		
4	Czech Republic	IT expert appointed security audit (50%) security certification (50%)	No details
5	Denmark	risk assessment (2/3) audit (2/3) security certification (1/3) CISO appointed vulnerability assessment (1/3) access to data is strictly restricted (id/pw) access log management (2/3)	access control through cards systems against intruders
6	Estonia	No specific procedures specific risk assesment (one case) internal audit no security certification CISO appointed (1 case) access to data is strictly restricted (id/pw) access log management (not all the companies) only partially encrypted	physically protected server rooms Limited access, fire alarm and break-in alarm

		Logical security measures	Physical security measures
Num	Countries		
7	Finland	Risk analysis IT security audits access to data is restricted (id/pw) no consolidated log handling for auditing purposes no encryption (only in transmission)	Yes Written procedures
8	France	No specific security for traffic data penetration test/vulnerability assessment access to data is strictly restricted (id/pw) access log management no encryption (only in transmission)	Alarms against intruders Access control through cards or special keys Closed Circuits TV Fire safety system for the servers and backups protection
9	Germany	<ul style="list-style-type: none"> • risk assessments • penetration tests • access to data is strictly restricted (id/pw) • access log management 	data centers are highly secured: <ul style="list-style-type: none"> • alarm • complete video surveillance • automatic fire extinguishing systems • etc...

		Logical security measures	Physical security measures
Num	Countries		
10	Greece	<p>access control, log files audit trail and use of secure communication channels</p> <p>general risk analysis</p> <p>Internal audits</p> <p>security certification (only one)</p> <p>CISO appointed</p> <p>independent penetration test/vulnerability assessment (30%)</p> <p>access to data is strictly restricted (id/pw)</p> <p>access log management (login-logout not actions)</p> <p>no encryption</p>	<p>no specific physical protection measures for traffic data.</p> <p>The physical protection measures are included in the general IT security policy.</p>
11	Hungary	<p>Regarding measures taken against unauthorized access it can be reported that all steps are logged, and IT systems are divided into basic, medium and high profile systems.</p>	<p>Servers are situated in a highly secured place, the entrance is secured by a proxy, hierarchic key, video surveillance and live security protection.</p>
12	Ireland	<p>Access to traffic data is restricted to limited number of users and logs of access are kept</p> <p>No specific studies in relation to security risks regarding traffic data</p> <p>Security certification</p> <p>CISO appointed</p> <p>Encryption in transmission</p>	<p>Data is stored on a number of dedicated system CCTV</p>

		Logical security measures	Physical security measures
Num	Countries		
13	Italy	<p>secure data transmission protocols; risk assessment; strong authentication; and the use of biometric tokens</p> <p>patch management procedures; use of anti-virus software; analysis of abnormal traffic via intrusion detection systems</p> <p>access log management</p> <p>no encryption (only in trasmission)</p>	<p>H24 monitoring;</p> <p>Access via badges;</p> <p>Centralised intrusion (detection) alarm;</p> <p>Video surveillance</p> <p>Fire detection systems;</p> <p>Restricted access areas</p>
14	Latvia	<p>the handling with traffic data is included in general IT security policy</p> <p>general IT audits</p> <p>External audits are selected only by large companies</p> <p>no operator has obtained a certification</p> <p>there aren't clear answers on regularity of tests carried out by providers</p> <p>only authorized persons have access to traffic data</p> <p>Almost 1/3 of providers are not recording the log files</p> <p>10% encrypted storage (all in transmission)</p>	<p>access control to facilities (secured by key code, magnetic cards etc.), video surveillance / monitoring, alarm systems, security staff/guards</p>

		Logical security measures	Physical security measures
Num	Countries		
15	Liechtenstein	internal audit company risk assessment no security certification CISO appointed access to data is strictly restricted (id/pw) access log management no encryption	secure data centre security personnel video surveillance intruder alarm system fire alarm system
16	Lithuania	Antivirus software, access to data is restricted, access log management, internal security, penetration tests(one company), audits (no audit in some cases), encryption (not in all cases), ISO 27001 certification (one company), CISO appointed, no IDS.	Entrance (Passing) control system (magnetic cards); premises surveyed by surveillance cameras; 24/7 hour security on duty; fire alarm sensors and automatic fire extinguisher system; continuous electric power supply
17	Luxembourg	No specific security for traffic data no risk assesment - security audit (only one) No operator is certified Encryption Access control and authentication Logs are not checked but only stored for investigation	Written policy (only two operators) IT security manager (only three) Access control through personnel cards Fire protection and intrusion detection systems. Storing of backups in a different place than the server itself (not all)

		Logical security measures	Physical security measures
Num	Countries		
18	Malta	<p>No specific security for traffic data</p> <p>internal audit/risk assesment</p> <p>CISO appointed (only one)</p> <p>no security certification</p> <p>IDS</p> <p>access to data is strictly restricted (id/pw)</p> <p>access log management</p> <p>encryption (only pw)</p>	<p>Access control through swipe cards</p> <p>Video Surveillance Closed Circuits</p> <p>Security Personnel</p> <p>Systems against intruders</p> <p>written policy</p>
19	Netherlands	<p>Risk assessments are part of the general IT security</p> <p>internal and external information security audits</p> <p>one operator 27001 certified</p> <p>CISO appointed</p> <p>vulnerability assessments on a regular basis</p> <p>access log management</p> <p>not all use encryption</p>	<p>Various physical security measures, e.g. all operators that were investigated store their traffic data in heavily secured data centres</p>
20	Poland	<p>None of them developed a separate IT security policy for traffic data</p> <p>information security risk analysis</p> <p>ICT security audits, both internal and external</p> <p>secirity certification</p> <p>CISO appointed</p> <p>intrusion detection/intrusion prevention systems</p> <p>access to data is strictly restricted (id/pw)</p> <p>access log management (inalterable in one case)</p> <p>no encryption (only in trasmission)</p>	<p>alarm system, CCTV, access control system</p> <p>isolated security zones</p> <p>redundant power supply</p> <p>fire alarm detectors</p>

		Logical security measures	Physical security measures
Num	Countries		
21	Romania	<p>There are companies that have adopted specific procedures for traffic data</p> <p>periodic risk assessment</p> <p>Only one company security certified</p> <p>No security manager</p> <p>No independent penetration test or vulnerability assessment</p> <p>access to data is restricted (id/pw)</p> <p>data base/system administrators are authenticated on the basis of user name and password</p> <p>log of primary activities (login, logout, change of password)</p> <p>no encryption</p>	<p>badges, video surveillance, anti seismic supports, fire detection and extinction system</p> <p>equipment are installed in specially arranged rooms</p> <p>no written policy</p>
22	Slovak republic	<p>IT security procedures directly applicable to the traffic data</p> <p>security audits and security analyses are performed regularly</p> <p>One company security certified</p> <p>CISO appointed</p> <p>independent penetration tests regularly</p> <p>access to data is strictly restricted (id/pw/token)</p> <p>access log management (except one)</p> <p>DB encryption (except two. all in transmission)</p>	<p>The entry is permitted for authorized persons only</p> <p>The policies are business secret; they may not be published nor given to external subjects</p>
23	Slovenia	<p>major providers: Information Security Management System (ISMS) adapted from ISO 27001 and dedicated Data Retention Solution (WORM CAS-type storage)</p>	<p>major providers: Information Security Management System (ISMS) adapted from ISO 27001 and dedicated Data Retention Solution (WORM CAS-type storage)</p>

		Logical security measures	Physical security measures
Num	Countries		
24	Spain	<p>No specific security for traffic data</p> <p>internal audits</p> <p>no security certification</p> <p>CISO appointed</p> <p>penetration tests</p> <p>IDS</p> <p>access to data is strictly restricted (id/pw)</p> <p>access log management</p> <p>no encryption (except one)</p>	<p>Access control through cards.</p> <p>Systems against intruders.</p> <p>Video Surveillance Closed Circuits.</p> <p>Alarm response centres.</p> <p>Security guards</p> <p>Written procedures</p>
25	UK	<p>No separate security procedures for traffic data</p> <p>risk assessments</p> <p>50% of organisations certified ISO 27001</p> <p>CISO appointed</p> <p>IDS</p> <p>access to data is strictly restricted (id/pw)</p> <p>access log management</p> <p>no encryption (only in trasmission)</p>	<p>Perimeter fencing.</p> <p>Secure hosting environments.</p> <p>Alarms.</p> <p>CCTV.</p> <p>Personnel access control systems</p> <p>24 hour police protection</p>

		Specific personal training for traffic data	Back up and disaster recovery	Data separation	Retention abroad
Num	Countries				
1	Belgium	Yes	back-up (100%) disaster recovery (50%)	YES	NO
2	Bulgaria	no details. The authorized persons that have access to the data are those responsible for: managing of traffic data, users' enquires, misuse detections, market studies and provision of added value services,requiring additional processing of traffic and localization data	back-up (100%) recovery systemes (no details)	YES	In accordance with the international agreement
3	Cyprus	Yes	back-up (100%) disaster recovery (only one no details)	YES (2/3)	NO

		Specific personal training for traffic data	Back up and disaster recovery	Data separation	Retention abroad
Num	Countries				
4	Czech Republic	Yes	contingency plan	YES	NO
5	Denmark	Yes	back-up (100%)	YES (2/3)	No
6	Estonia	not specific	back-up copies are taken centrally, existing policy for rotating back-up copies, automatically administrated lifecycle of back-up copies	yes, data are separated phisically and logically in different databases	only one case but situated in EEA

		Specific personal training for traffic data	Back up and disaster recovery	Data separation	Retention abroad
Num	Countries				
7	Finland	Yes	Back up	No	No
8	France	not specific	back-up (100%) recovery systemes (no details)	YES	NO
9	Germany	Yes	back-up systems – some actually in encrypted form	YES	NO

		Specific personal training for traffic data	Back up and disaster recovery	Data separation	Retention abroad
Num	Countries				
10	Greece	not specific	back-up (100%) recovery systemes (no details)	NO	ONE CASE WITHIN EU
11	Hungary	classified data requests are compiled by a person having passed the „C” type national security clearance. In case of open data requests, most of the companies organise compulsory tranings about the specific knowledge	only a few comanies have their own recovery plan but first they were not willing to show these documents. Many companies have security archiving separeted from the servers	most of the companies store the data related to invoices logically or physically separated from the data stored in connection with criminal investigations	No
12	Ireland	Yes	Back-up (1001%) No specific continuity / disaster recovery procedures in place for traffic data	No	No

		Specific personal training for traffic data	Back up and disaster recovery	Data separation	Retention abroad
Num	Countries				
13	Italy	Yes	back-up (100%) recovery systemes	Yes	No
14	Latvia	not specific	The back-up system is implemented by 81 % of providers few small providers that do not have back-up systems in operation	62 % do not separate the data	Yes (in EU)

		Specific personal training for traffic data	Back up and disaster recovery	Data separation	Retention abroad
Num	Countries				
15	Liechtenstein	Yes	back-up (100%) recovery systemes (50%)	Yes (50%)	Yes
16	Lithuania	not specific	back-up (100%) recovery systems (except 1 company)	Yes, data are stored separately	One company providing mobile telephony services stores traffic data not only in Lithuania, but also in others EEA countries (Latvia, Estonia, Sweden)
17	Luxembourg	Yes (not all)	Operators use back-up systems. Copies are deleted by overwriting in a general rotation of supports. There are no formal Business Continuity Process in place. Three operators however, store backup on a remote site.	Yes (only two)	All operators store all their data in Luxembourg, except for two that also store some data in Belgium

		Specific personal training for traffic data	Back up and disaster recovery	Data separation	Retention abroad
Num	Countries				
18	Malta	Yes	Only one operator has back-up procedures	Yes (not all)	Yes (in EU)
19	Netherlands	Handling of traffic data for law enforcement purposes is done by specific group of personnel.	Different strategies, e.g. parallel processing at two different locations	3 telecom providers that were investigated store, or are planning to store, the traffic and location data that is retained under the TLC Data Retention Act in separate databases.	Data that is retained under the Telecommunications Data Retention act is stored, or will be stored, in the Netherlands
20	Poland	Yes	back-up (100%) disaster recovery (only one no details)	NO	NO

		Specific personal training for traffic data	Back up and disaster recovery	Data separation	Retention abroad
Num	Countries				
21	Romania	Yes	periodic backup, DR equipment located in another city in "hot back up". The backs up copies are in constant synchronisation	Yes	No
22	Slovak republic	Yes	back-up (100%) recovery systemes	Yes	Yes (in EU)
23	Slovenia	Yes	Yes	Yes	No

		Specific personal training for traffic data	Back up and disaster recovery	Data separation	Retention abroad
Num	Countries				
24	Spain	Yes	back-up (100%) recovery systemes (except one)	Yes	No
25	UK	not specific	back-up (100%) recovery schemes (off-site back up)	Mixed situation with some physical separations already in place and one being implemented	NO