



**Quarterly newsletter on
European Regulatory Issues**

July 2008

TABLE OF CONTENTS

I.	DATA RETENTION DIRECTIVE	3
1.	Overview of Legislation	3
a.	Objectives and scope	3
b.	Requirements	3
c.	Impact on PRISM	5
2.	Developments	5
3.	Next steps	6
4.	Implementation Process.....	7
a.	National legislation and key issues	7
5.	PRISM Strategy	13
6.	Useful links.....	14
7.	Key actors on EU level	14
II.	8TH COMPANY LAW DIRECTIVE	15
1.	Overview of Legislation	15
a.	Objective and scope	15
b.	Requirements	15
c.	Impact on PRISM.....	16
2.	Recent developments	16
3.	Next steps	16
4.	PRISM strategy	17
5.	Useful links.....	17
6.	Key actors on EU level	17
III.	CAPITAL REQUIREMENTS DIRECTIVE (BASEL II)	18
1.	Overview of Legislation	18
a.	Objectives and scope	18
b.	Requirements	18
c.	Impact on PRISM.....	20
2.	Recent developments	20
3.	Next steps	20
4.	Implementation Process.....	21
a.	National legislative and regulatory framework	21
c.	Possible changes to the CRD	22
5.	PRISM strategy	23
6.	Useful links.....	23
7.	Key actors on EU level	23
	ANNEXES.....	24

I. DATA RETENTION DIRECTIVE

1. Overview of Legislation

a. Objectives and scope

On 15 March 2006 the European Union formally adopted [Directive 2006/24/EC](#), 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".

It aims to **harmonise Member States' provisions** concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by Member States in their national law.

b. Requirements

The Directive applies to **traffic and location data** on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It **does not apply to the content of electronic communications**, including information consulted using an electronic communications network.

Member States also have to ensure that the retained data is provided on request **only to the competent authorities** under conditions defined by national legislation.

The following **categories of data** must be retained with regard to fixed network telephony and mobile telephony, as well as Internet access, Internet e-mail and Internet telephony:

- data necessary to trace and identify the source of a communication;
- data necessary to trace and identify the destination of a communication;
- data necessary to identify the date, time and duration of a communication;
- data necessary to identify the type of communication;
- data necessary to identify the communication device;

- data necessary to identify the location of mobile communication equipment.

Member States must ensure that the categories of data specified are retained for **periods of not less than six months and not more than two years** from the date of the communication. A Member State facing particular circumstances that warrant an extension for a limited period of the maximum retention period may take the necessary measures. That Member State shall immediately notify the Commission and inform the other Member States of the measures taken and state the grounds for introducing them. The Commission shall, within a period of six months after the notification, approve or reject the national measures concerned, after having examined whether they are a means of arbitrary discrimination or a disguised restriction of trade between Member States and whether they constitute an obstacle to the functioning of the internal market. In the absence of a decision by the Commission within this period the national measures shall be deemed to have been approved.

The Directive goes on to make provision for **data protection and data security**. Each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, certain prescribed data security principles with respect to data retained in accordance with the Directive. Each Member State must designate a supervisory authority to be responsible for monitoring the application within its territory of the provisions adopted by the Member States regarding the security of the stored data. Those authorities may be the same authorities as those referred to in Article 28 of Directive 95/46/EC. The supervisory authority must act with complete independence.

The directive also includes the establishment of a relevant **working group** meant to advise and share best practices in data retention. PRISM EU office has already contacted European Commission officials regarding a possible participation. The association will however not be invited to become a member of the experts group since PRISM does not fall within one of the target categories (Member States' law enforcement authorities, associations of the electronic communications industry, representatives of the European Parliament and data protection authorities, including the European Data Protection Supervisor). It would remain possible for PRISM to be invited to participate at particular discussions of the experts group where their knowhow and experience could contribute to these discussions.

c. Impact on PRISM

The directive also sets **storage requirements** for the retained data. In this sense, data requested by the authorities has to be transmitted as soon as possible. Data storage companies play therefore an important role in the overall compliance with the directive for the telecommunications companies.

2. Developments

15/09/2007	<p><u>Transposition deadline</u></p> <p>Member States have the obligation to transpose the provisions of the directive into national law, otherwise the European Commission may call the respective state in front of the Court of Justice for not respecting its obligations.</p> <p>20 Member States did not meet the deadline.</p>
26/11/2007	<p>The Commission issued <u>Letters of Formal Notice</u> to those Member States, which had not at that date notified their national transposition measures. These letters were sent to Bulgaria, Germany, Estonia, Ireland, Greece, Italy, Cyprus, Lithuania, Luxembourg, Hungary, Malta, the Netherlands, Austria, Poland, Portugal, Romania, Slovenia, Slovakia, Finland and Sweden.</p>
<p>30/11/2007</p> <p>Link to document</p>	<p><u>Transposition issues</u></p> <p>The Commission invited all Member States to a meeting in order to discuss transposition issues surrounding the Directive. The roundtable discussion revealed that in the majority of cases, delays were due to the length of discussions in national parliaments.</p>
<p>22/01/2008</p> <p>Document available Annex 1.1</p>	<p>MEP Alexander Alvaro (ALDE Group, Germany) and Marco Cappato (ALDE Group, Italy) ask to the Commission to illustrate the transposition process in Member States of the directive.</p>
14/02/2008	<p>The European Commission answered the question giving the following overview:</p> <ul style="list-style-type: none"> - the deadline of transposition was 15 September 2007

<p>Document available Annex 1.2</p>	<ul style="list-style-type: none"> - a derogation is possible for data relating internet if a Member State makes a declaration to postpone application for a further 18 months period (18 States made a declaration to postpone the adoption until 15 March 2009) - on 26 November 2007 the Commission issued letters of formal notice to 20 Member States - Since the Letters of Formal Notice were issued, Germany, Estonia, Cyprus and Slovakia have notified their transposition measures and the other States are in the process of notifying them - The European Commission is presently assessing the notified measures.
<p>June 2008</p>	<p>No further action has been taken by the European Commission on infringement procedures against Member States.</p>

3. Next steps

<p>As soon as possible</p>	<p>Finalisation of transposition in all Member States</p>
<p>15/03/2009</p>	<p>Deadline on transposition of requirements relating to Internet Access, Internet telephony and Internet e-mail.</p> <p>Any Member State that intends to make use of this provision must notify the Council and the Commission to that effect by way of a declaration. At the entry into force of the directive, the following 18 Member States made such a declaration postponing application for differing lengths of time: the Netherlands, Austria, the United Kingdom, Estonia, Cyprus, Greece, Luxembourg, Slovenia, Sweden, Lithuania, Latvia, Czech Republic, Belgium, Poland, Finland, Germany, Romania and Bulgaria.</p>
<p>15/09/2010</p>	<p>The Commission must submit an evaluation of the application of the Directive and its impact on economic operators and consumers, taking into account further developments in electronic communications technology and the statistics provided to the Commission with a view to determining whether it is necessary to amend the provisions of this Directive, in particular with regard to the list of data and the periods of retention.</p>

4. Implementation Process

a. National legislation and key issues

Transposition process

In order to be effective all European directives have to be transposed in the law of each Member States which have the full responsibility for this. The laws transposing the directives must fulfill the directives requirements and must be carried out within the time limits laid down by the directives themselves. The transposition process starts as soon as the directives entry into force (after 20 days from the publication of the directives in the Official Journal) and Member States shall bring into force the provisions necessary to comply with the directives. In the case of the Data Retention Directive Member States had until 15 September 2007 to transpose the directive into national law and until 15 March 2009 with regard to the part of the directive related to internet traffic.

Reimbursement of costs

In transposing European legislation into national law, Member States have to follow the objective and the requirements imposed by directives. However in the case of the Data Retention Directive they had freedom of decision in regard to the reimbursement of the costs paid by Telco companies to fulfill the requirements imposed by the directive (the storage of data). A Member State can decide to reimburse the expenses incurred by a telecommunication provider in complying with national legislation imposing to store data.

Overview of Data Retention Directive transposition in Member States

Member State	Transposition Law	Reimbursement	Key issues
AUSTRIA	Draft proposal	No	<ul style="list-style-type: none"> In July 2007, the Austrian government confirmed that the data retention transposing law would not be ready before the deadline set by the directive, due to the large number of responses to the public consultation on this issue.
BELGIUM	Draft proposal	Under discussion	
BULGARIA	Not available		
CYPRUS	Not available	No	
CZECH REPUBLIC	Draft proposal	Foreseen in the proposal which is currently under discussion	<ul style="list-style-type: none"> Draft act amending the Electronic Communications Act (127/2005) is now pending in the Senate. The act is close to approval.
DENMARK	Administrative order approved on 28 September 2006	No	<ul style="list-style-type: none"> The Act providing for data retention was approved by the Danish Parliament already in June 2002 as part of the Danish "anti-terrorism package" The administrative order regulates in more details the obligations of the telecommunications providers and further implements the recently adopted EU Directive on Data Retention For fixed lines and mobile phones (including voice, voicemail, call forwarding, conference calls, SMS, MMS) the retained data are: phone number, user ID (e.g. customer number), name and address of customer, IMSI / IMEI number, unsuccessful call attempts, first and last cells ID and physical location (mobile communication), and date and time for start and end of communication.

			<ul style="list-style-type: none"> For Internet use, the retained data are session logging (first and last or every 500 package), IP address, port number and transport protocol, user ID, phone number for dialup access, location and ID of hot spots, date and time for start and end of communication.
ESTONIA	<p>Law came into force 1 January 2008</p> <p>15 March 2009 as for the internet data</p>	No	<ul style="list-style-type: none"> Data retention period: 12 months. Estonia decided not to compensate the data retention costs for the telcos but only the costs that are related to the provision of the information to the surveillance agencies or security authorities are compensated.
FINLAND	Draft proposal	Under discussion	
FRANCE	<p>“Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques”</p> <p>Link to document</p>	<p>Reimbursement of costs incurred only for retrieval, no provisions on general data retention costs.</p> <p>In practice the State is not paying companies.</p>	<ul style="list-style-type: none"> It requires telecommunication data operators (Internet and telephony) to retain data for one year. Concerned data are those allowing the identification of: <ul style="list-style-type: none"> the user and its terminal equipment the recipients of the communication the date, time and duration of the communication the additional services used and their suppliers the origin and the location of the communication (for telephony services)
GERMANY	<p>Law adopted on 10 November 2007</p> <p>Link to document</p>	No	<ul style="list-style-type: none"> Traffic data accessible not only for criminal prosecution purposes, but also in order to "prevent considerable dangers" and "fulfill the legal duties" of all security police Entered into force on 1 January 2008 All telecommunication providers will be requested to keep the traffic data for six months For the Internet services, this obligation

			<p>will start at the beginning of 2009. The Internet traffic data will include storing the email addresses, IPs and time stamps in the case of electronic mail.</p> <ul style="list-style-type: none"> It is important to note that great public opposition took place in Germany during the legislative process of this law – public manifestations, communication platforms, official demand for suspension of the law at the Federal Constitutional Court
GREECE	Not available		
HUNGARY	Draft proposal	No	
IRELAND	Draft proposal	No	<ul style="list-style-type: none"> Irish Government intends to implement the Data Retention Directive by an order of a Minister rather than legislation passed by Parliament. June 2008: government proposal to extend data retention to internet (storage period: 12 months)
ITALY	<p>Act approved on 21 May 2008</p> <p>Published on 18 June 2008</p> <p>In force as from 3 July 2008</p> <p>Link to document</p>	No	<ul style="list-style-type: none"> Telephone traffic data must be retained for 24 months For unsuccessful calls data retention period is 30 days Public authorities can ask to internet service providers and phone company to retain data (excluding the content) for maximum 90 days for investigative reasons. Fine: from 10.000 to 50.000 Euro which can be increased to 150.000 in relation to economic conditions of the violating company.
LATVIA	<p>Into force as from 15 March 2009</p> <p>Document available Annex 1.3</p>	No	<ul style="list-style-type: none"> Retention period of 18 months.

	Annex 1.4		
LITHUANIA	Draft proposal	Under discussion Reimbursement is the main issue blocking the vote of the law	<ul style="list-style-type: none"> The directive is not transposed yet. Law on Electronic Communications (transposing the directive) received the veto from the President of the Republic of Lithuania sending the law back to the Government.
LUXEMBURG	Not available		
MALTA	Not available		
HOLLAND	Draft law on 21 December 2006	Costs are still an issue and cost estimates are still vague. General costs will not be reimbursed	<ul style="list-style-type: none"> The final text lowered the retention period to 12 months, both for telephone and Internet traffic data. At first data will be stored directly by the providers but this could change in the future.
POLAND	Not available		
PORTUGAL	Not available		
ROMANIA	<p>Draft law adopted on 20 February 2008 Link to document</p> <p>June 2008 Senate approved it</p> <p>Possible approval by Parliament October 2008</p>	No	<ul style="list-style-type: none"> Data should be retained for one year. The obligation to retain the data is only for electronic communication operators, thus excluding information society service providers. The retained data can be accessed by prosecutors only in the penal cases related to organized crime and terrorism crimes and with a proper specific judge-approved access authorization. According to the draft, the Internet-related data will be kept only starting with 15 March 2009
SLOVAKIA	Law adopted 29 December 2007	No	
SLOVENIA	Not available		
SPAIN	Draft law approved 21	No	<ul style="list-style-type: none"> The draft law on the retention of traffic data requires fixed and mobile

	<p>June 2007</p> <p>Published on 19 October 2007</p> <p>Entered into force November 2007</p> <p>Document available Annex 1.5</p>		<p>telephony, but also ISPs to retain data for a period of one year and to make it available to law enforcement or secret services under court order</p> <ul style="list-style-type: none"> The pre-paid mobile telephone cards will no longer be anonymous, the telephony operators being obliged to register the data of the pre-paid customers. In case of the cards already sold before the entering into force of the law, operators are bound to gather the information on the card owners during a period of one year and when this is not possible, the cards must be disconnected and cancelled.
SWEDEN	Not available	Under discussion Commission of inquiry proposes that authorities on a case by case basis have to reimburse costs when providers supply them with retained data.	<ul style="list-style-type: none"> A commission of inquiry has examined the transposition and submitted a report on its conclusions. The report has been circulated for comments among relevant stake holders and ministry is currently working on drafting a bill. The new bill will have to be approved by the Parliament. The approved law is expected to come into force in early 2009.
UK	<p>Law adopted 24 July 2007 “The Data Retention (EC Directive) Regulations 2007 No. 2199”</p> <p>Link to document</p>	<p>Yes</p> <p>Both running costs and capital costs will be reimbursed after the approval of the Secretary of State</p>	<ul style="list-style-type: none"> the law applies only to telecom companies that will have to preserve phone call logs for one year, but does not apply to Internet traffic data such as emails, web surfing or VoIP phone calls came into force on 1 October 2007 for Internet traffic data, UK will take advantage of the delay until March 2009 to propose measures, the bill is likely to follow the present regulation imposing a data retention period of 12 months.

5. PRISM Strategy

PRISM considers the data retention directive as the main priority EU legislation. The transposition in the Member states and practical implementation will be constantly monitored and reported in the quarterly newsletters.

a. Network

Kellen Europe is compiling a list of contact persons both at national and European level dealing with the transposition of the directive. This list is a “living document” and will be updated on an ongoing basis. The objective is that PRISM Intl members have a contact person in their respective Member State/of their Permanent Representation in case they have any questions on the implementation and compliance with the Data Retention Directive.

PRISM EU office is in close contact with the European Commission (Nicholas Kaye) and with the Member of the European Parliament (MEP) Alvaro.

b. Workshop

In addition PRISM Intl is in the process of organizing a workshop on the Data Retention Directive with the support of MEP Alexander Alvaro. PRISM EU office is currently defining the date of the workshop and the involvement of ETNO (European Telecommunications Network Operators Association).

The objective of the workshop will be to provide telecommunication companies/ISPs with the opportunity of having a discussion on the implementation of the data retention. The workshop will be a unique chance for PRISM Intl explaining both to telcos/ISPs and to policy makers the opportunity to outsource the data storage.

6. Useful links

European Commission – Justice and Home Affairs – [website](#)

European Parliament – Committee on Civil Liberties, Justice and Home Affairs – [website](#)

Justice and Home Affairs Council – [website](#)

European Data Protection Supervision – [website](#)

7. Key actors on EU level

European Commission

Nicholas KAYE

Administrator

Directorate General Justice, Freedom and Security

Directorate D: Internal security and criminal justice

Unit D1: Fight against terrorism, and access to information

II. 8TH COMPANY LAW DIRECTIVE

1. Overview of Legislation

a. Objective and scope

The 8th Company Law Directive (on Statutory Audits of Annual and Consolidated Accounts) updates provisions of the earlier Audit Directive and introduces new provisions on public oversight, third country auditors and various other matters.

[Directive 2006/43/EC](#) of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/ 660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC, aims to complete the series of Directives concerning company accounts, **defining the qualifications of persons responsible for carrying out the statutory audits of the accounting documents required by the fourth and seventh Directives.**

b. Requirements

The directive lays down **minimum requirements and fundamental principles for statutory auditing**. The directive attempts to reach high-level harmonization of statutory audit requirements in the areas of competence, qualifications, training, ethics, objectivity, standards and others.

The directive insists on the **respect of privacy and confidentiality concerning data collected** by the auditors and audit firms. Audit firms are also responsible for the carrying out of their work in respect of the principles mentioned above.

Member States authorities in charge with approval, registration and inspections of the audit firms must also pay special attention to the **handling of data** they gather in the course of their activities.

To ensure the protection of interests of 3rd parties, a **publicly accessible register of auditors and auditing firms** is proposed. In this respect, the public interest function of statutory auditors plays a major role. The European Commission attempts to set minimum standards for professional ethics, confidentiality, professional secrecy and the independence of statutory auditors.

Auditing firms are also required to create and publish **transparency reports** on their activities on an annual basis.

In order to use statutory audits, the Community requires consistent high quality in all audits. The harmonization of international auditing standards will significantly contribute to this requirement. The international auditing standards developed by the European Commission are accepted internationally by an open and transparent procedure. To ensure such high quality statutory audits, the directive recommends Member States to organize a **system of quality assurance**. Public oversight of the Member States and regular inspections can play a large role.

c. Impact on PRISM

The directive affects all listed companies that undergo audits, especially in the banking sector – PRISM members might be faced with record storage demands coming from companies that need to comply with the directive.

Because of the 8th directive in force, there is an increase in company records, which also leads to an increase in auditing records.

2. Recent developments

17/05/2006	Final legislative act - 2006/43/EC
09/06/2006	<u>Publication in the Official Monitor</u> - Entry into force – 20 days after the publication

3. Next steps

29/06/2008	<u>Transposition deadline</u> EU Member States must comply with this Directive before this deadline.
July/August 2008	The European Commission is currently receiving notifications from Member States on their implementation laws. A first "Scoreboard" of the implementation of the 8th Directive will be published in July/August 2008, describing where Member States stand.

4. PRISM strategy

The 8th Company Law Directive was identified as the second EU legislation priority. Since the transposition deadline for this directive is end of June 2008, any future issues regarding the national situations will be included when the case in the next issues of the newsletter.

PRISM EU office has established contact with desk officer in the European Commission.

5. Useful links

European Commission – Internal Market – [website](#)

European Parliament – Committee on Internal Market and Consumer Protection – [website](#)

Competitiveness Council (Internal Market, Industry and Research – [website](#))

6. Key actors on EU level

European Commission:

Jürgen Tiedje
Head of Unit

Ms. Majewska
Policy officer

DG Internal Market and Services
Directorate F: Free movement of Capital, Company Law and Corporate Governance
Unit F4 Auditing

III. CAPITAL REQUIREMENTS DIRECTIVE (BASEL II)

1. Overview of Legislation

a. Objectives and scope

The **Basel II framework** (international recommendations on banking laws and regulations issued by the Basel Committee on Banking Supervision) is to be **implemented in the EU through the Capital Requirements Directive (CRD)** – made up of two directives: 2006/48/EC relating to the taking up and pursuit of the business of credit institutions and 2006/49/EC on the capital adequacy of investment firms and credit institutions.

b. Requirements

The Capital Requirements Directive ([2006/48/EC](#) and [2006/49/EC](#)) affects all banks (or credit institutions - CI) and certain types of investment firms. It is more **risk-sensitive** and sets rules for:

- Three different levels from which institutions can choose (*Pillar 1*): standard, foundation and advanced;
- *supervisory review process (Pillar 2)*: CIs do an internal assessment which is then checked by supervisors and the minimum required amount of capital is set (capital charge);
- *public disclosure (Pillar 3)*: CIs must make certain information public to allow the market to judge their risk worthiness and react accordingly (market discipline);
- *single market passport*: mutual recognition system allowing banks and CIs to operate throughout the EU once approved by their own national regulatory authority, and;
- *consolidating supervisor*: a new national banking supervisory body responsible for **cross-border issues**. It must ensure harmonisation across the single market.

In the text of the directive, special attention is given to the **data used in the estimations** that credit institutions produce in order to assess credit risk.

Credit institutions should be capable to produce relevant data and information requested by competent authorities:

Credit institutions may be given explicit permission by the competent authority to calculate their risk-weighted exposure amounts using the Internal Ratings Based Approach ('IRB Approach'). Permission can be given only if the competent authority is satisfied that the credit institution's systems for the management and rating of credit risk exposures are sound and implemented with integrity and they meet the several standards, among which the collection and storage of all relevant data in order to provide effective support to its credit risk measurement and management process.

A special chapter of Annex VII of the directive refers to **data maintenance**. Credit institutions are to **collect and store various types of data**:

- (a) complete rating histories on obligors and recognised guarantors;
- (b) the dates the ratings were assigned;
- (c) the key data and methodology used to derive the rating;
- (d) the person responsible for the rating assignment;
- (e) the identity of obligors and exposures that defaulted;
- (f) the date and circumstances of such defaults; and
- (g) data on the PDs and realised default rates associated with rating grades and ratings migration;

- (a) complete histories of data on the facility ratings and LGD and conversion factor estimates associated with each rating scale;
- (b) the dates the ratings were assigned and the estimates were done;
- (c) the key data and methodology used to derive the facility ratings and LGD and conversion factor estimates;
- (d) the person who assigned the facility rating and the person who provided LGD and conversion factor estimates;
- (e) data on the estimated and realised LGDs and conversion factors associated with each defaulted exposure;
- (f) data on the LGD of the exposure before and after evaluation of the effects of a guarantee/or credit derivative, for those credit institutions that reflect the credit risk mitigating effects of guarantees or credit derivatives through LGD; and
- (g) data on the components of loss for each defaulted exposure.

- (a) data used in the process of allocating exposures to grades or pools;
- (b) data on the estimated PDs, LGDs and conversion factors associated with grades or pools of exposures;
- (c) the identity of obligors and exposures that defaulted;

- (d) for defaulted exposures, data on the grades or pools to which the exposure was assigned over the year prior to default and the realised outcomes on LGD and conversion factor; and
- (e) data on loss rates for qualifying revolving retail exposures.

c. Impact on PRISM

Financial institutions have to comply with the measures of the accord and on the EU territory with the abovementioned directives and are responsible for their actions when it comes to outsourcing activities. Increased obligations for financial institutions mean an increase in quantity of records and increased need for records' storage and management.

2. Recent developments

14/06/2006	<u>Final legislative act</u> - 2006/48/EC & 2006/49/EC
30/06/2006	<u>Publication in the Official Monitor</u> - Entry into force – 20 days after the publication
31/12/2006	<u>Transposition deadline</u> The deadline for transposition into national law was 31 December 2006.

3. Next steps

2007-2008	<u>Implementation</u> Member States are to apply the Directive from the start of 2007, with the most sophisticated approaches being available from 2008. This is in line with the planned global introduction of the Basel II rules.
-----------	--

4. Implementation Process

a. National legislative and regulatory framework

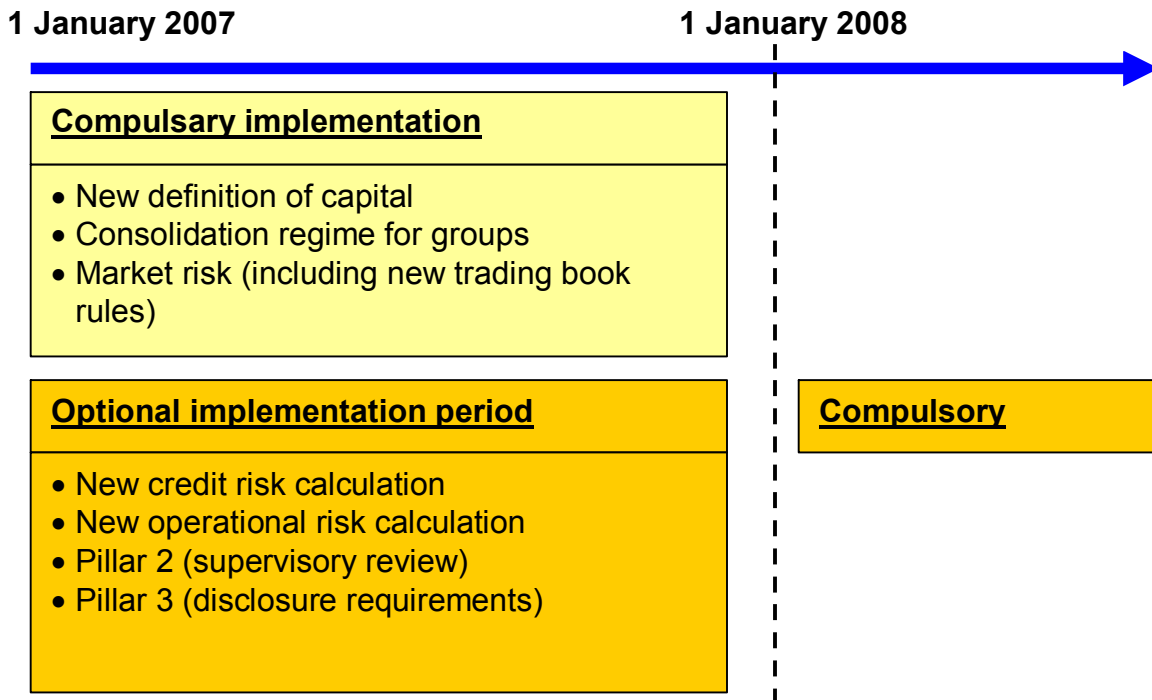
The Commission set up a specific working group – the Capital Requirements Directive Transposition Group (CRDTG) (representatives from the European Commission and Member States). The objective of the group is to facilitate correct and coherent transposition of the CRD in Member States legislation. In particular, the CRDTG will provide all interested parties with interpretations on the CRD and to make them available on the websites of the Commission and of the Committee of European Banking Supervisors (CEBS) – see “Useful links”. The CEBS provides a detailed overview of the transposition laws in and regulations in the Member States, as well as in Iceland, Lichtenstein and Norway.

[Overview transposition 2006/48/EC](#)

[Overview transposition 2006/49/EC](#)

b. CRD Implementation Timeline

2007 has been a transitional year for CRD implementation. A two-stage process for the national implementation of the CRD began with the bulk of the rules taking effect on 1 January 2007 (for optional 'early adoption' during 2007 and full adoption on 1 January 2008), and the remainder of the rules took effect on 1 January 2008. Firms were able to elect to remain on the Basel I framework throughout 2007 and, in practice, the majority of firms chose to do so, while preparations for full implementation were being put in place. From European Commission sources we have been told that **all the Member States have fully transposed the CRD**. Currently the European Commission is verifying the practical functioning of the transposing laws, in case of problems it will inform the State concerned.



c. Possible changes to the CRD

On the 16 April 2008 the European Commission has launched a public consultation on possible changes to the CRD (2006/48/EC and 2006/49/EC). The purpose of this consultation was to collect comments of the industry and other stakeholders on these modifications. The European Commission is also conducting an impact assessment related to the modification of certain provisions. Stakeholders have been invited to give the European Commission their views on the issues by 16 June 2008. Opinions have been sought on: (i) large exposures, (ii) hybrid capital instruments, (iii) supervisory arrangements, (iv) the waivers for banks organised in networks and (v) adjustments to certain technical provisions.

The responses to the consultation will provide guidance to the European Commission for the preparation of a proposal that is scheduled to be adopted in September 2008.

5. PRISM strategy

The Capital Requirements Directive is the third selected priority EU legislation. PRISM will continue to monitor and report on the developments via the quarterly newsletter.

PRISM EU office has established contact with desk officer in the European Commission and with a counterpart within a European Banking federation/association.

6. Useful links

European Commission – Banking [website](#)

Committee of European Banking Supervisors (CEBS) – general [website](#); Capital Requirements Directive Transposition Group (CRDTG) [website](#)

European Commission & CEBS – queries and responses [website](#)

European Parliament – Committee on Internal Market and Consumer Protection – [website](#)

Competitiveness Council (Internal Market, Industry and Research – [website](#))

7. Key actors on EU level

European Commission:

Patrick Pearson
Head of Unit

Arvind Wadhwa
Deputy Head of Unit

DG Internal Market and Services
Directorate H: Financial Institutions
Unit H1: Banking and Financial Conglomerates

European Banking Federation

Florence Ranson
Senior Adviser
Information and Communication

Valeria Messina
Adviser
Information and Communication

ANNEXES

DATA RETENTION DIRECTIVE

Annex 1.1 – Written Parliamentary Question

Annex 1.2 – Written Answer by the European Commission to Parliamentary Question

Annex 1.3 – Latvian transposition law - December 2007

Annex 1.4 – Latvian Electronic Communications Law - May 2007

Annex 1.5 – Spanish transposition law – October 2007