European Financial Markets Lawyers Group

- THE CHAIR -

CONFIDENTIAL

Mr Jonathan Faull
Director General
DG Internal Market and Services
European Commission

Mr Martin Merlin
Director
Directorate Financial Markets
DG Internal Market and Services
European Commission

Mr Mario Nava
Director
Directorate Financial Institutions
DG Internal Market and Services
European Commission

Mr Adam Farkas
Executive Director
European Banking Authority

Mr Piers Haben
Director
Oversight Department
European Banking Authority

Mrs Isabelle Vaillant
Director
Regulation Department
European Banking Authority

30 October 2014

Dear Sirs,

Dear Madam,

Banking Secrecy

As you may know, the European Financial Markets Lawyers Group is a group of senior legal experts from the EU banking sector dedicated to making analysis and undertaking initiatives intended to foster the harmonisation of laws and market practices and facilitate the integration of financial markets in Europe. The Groups is hosted by the European Central Bank[1].

This letter aims to make you aware of a potential dilemma European financial institutions might face resulting from the various applicable banking secrecy laws[2] as a consequence of banking groups'

[1] More information about the EFMLG and its activities is available on its website at www.efmlg.org.

[2] For the purpose of this letter, "banking secrecy law" will refer to confidentiality obligations and disclosure constraints arising under the regulations protecting a country's sovereignty (e.g. so-called "blocking laws/statutes"): laws of banking secrecy and the specific duties of confidentiality that have been developed

international presence on the one hand and new regulations requesting transaction based information or stipulating a group wide risk management approach on the other hand. Financial institutions have to deal with an increased pressure to comply with several (foreign) laws and other regulatory requests for access to data, potentially conflicting with the various applicable banking secrecy laws which may constrain such disclosures in the countries in which they operate.

Fragmented and divergent banking secrecy regimes in the EU

Banks have to observe banking secrecy in almost all European countries[3]. However, banking secrecy rules are neither harmonised in scope, format nor consequences in case of breach[4]. Against this backdrop, the absence of a harmonised legal framework and the consequent heterogeneous picture of banking secrecy legislation in the EU, might cause legal uncertainty, especially in view of the ever increasing regulatory obligations affecting it.

Specifically, the wide range of banking secrecy laws have proved to create excessive constraints for financial institutions with a group wide presence or cross border activities. They often encounter legal[5] and reputational risks when passing on information within a group as local banking secrecy laws often do not foresee an "intra-group exemption" while being obliged, at the same time, to share some information for prudential or anti-money laundering purposes. Hence it is clear that those financial institutions may be subject to various applicable banking secrecy rules, which in most cases leads, in practice and due to caution, to the cumulative application of legal regimes.

Transaction reporting and information sharing

One of the most recurring problems that financial institutions are currently confronted with is that they are required to comply with several reporting requirements for derivative transactions that are imposed by foreign regulations. The Dodd Frank Act[6] for example requires swap dealers and major swap participants to report comprehensive transaction and counterparty data of swap transactions to regulators or trade repositories. Many financial institutions expressed their concern that a complete compliance would be

---

through either case law, legislation or otherwise. Personal data protected under a data protection regime, consumer protection rules and IT security constraints are left out of the scope of this letter.

3 A survey held amongst the members of the EFMLG confirmed that almost all of the jurisdictions surveyed have either a statutory or regulatory privacy/ confidentiality obligation that may apply (with the exception of the Netherlands). Even if local law remains silent on this point there might exist an implied duty of confidentiality. This study has also demonstrated that there is no harmonised European Union regime as the national laws/practices have not arisen out of a Directive or other European Union regulations. For further details see Annex 1a to this letter.

4 In many of the jurisdictions express written consent of the counterparty will be sufficient to remove the applicable banking secrecy law prohibition, but that in some jurisdictions this consent is not sufficient.

5 I.e. non-compliance might give cause to civil damages and/or criminal sanctions. A table of exemptions /deep-dive for selected jurisdictions is attached as Annex 1b. "Compliance risk" is defined as the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its banking activities (together, "compliance laws, rules and standards"). See Basel Committee on Banking Supervision, Compliance and the compliance function in banks (2005), p.7 [http://www.bis.org/publ/bcbs113.pdf].

6 A similar requirement has been imposed by the European Market Infrastructure Regulation (EMIR).

difficult to achieve due to the existing national banking secrecy laws. A recent letter from the ODRG to the FSB confirmed these concerns[7].

As explained before, in some countries (such as France), a less strict banking secrecy regime has been adopted, allowing the transfer of information without the consent of the client under certain conditions towards persons with whom they are engaged in the negotiation, conclusion or execution of certain transactions such as transactions on financial instruments (e.g. CDS), guarantee or insurance for credit risk coverage purposes, or assignment or transfer of receivables (e.g. disclosure of information is permitted on a need to know basis). These exceptions enable, in most cases, compliance with the operational requirements of the "Originate To Distribute" (OTD) model, which implies the sharing of information with investors (insurance companies, investment funds etc.). As said previously, it is however necessary to check this possibility in all countries concerned (for cross-border transactions).

Most of the European regimes recognize the bank's right to provide information covered by banking secrecy only to a limited number of listed authorities, including prudential authorities, market authorities, tax offices and judicial authorities. Conversely, the bank cannot provide information to foreign authorities without the client's approval.

Group-wide Risk Management & deep-dive reporting obligations

Another key challenge for financial institutions is the increase of regulations that require a group wide risk management and demand a data transfer for a consolidated view.

The BCBS Principles for an Effective Risk Data Aggregation and Risk Reporting practices (Paper BCBS #239), to be implemented by the G-SIBs by 1 January 2016, for example, require to "*enhance the management of information across legal entities, while facilitating a comprehensive assessment of risk exposures at the global consolidated level*". This has resulted in the fact that in recent years many financial institutions began to centralise certain databases and processes for risk management or efficiency purposes, as a consolidated risk management obliges them to coordinate their related activities on a group wide basis across the head office, branches and subsidiaries.

In this context, we would also like to make reference to the reporting obligations that have been imposed by the Financial Stability Board, pursuant to its macro-prudential supervision of systemic institutions. This implies frequent reporting, including in particular the provision of the list of counterparties, without the law providing a waiver of professional privilege in its favour (FSB Data Gaps Initiatives: a Common Data Template for Global Systemically Important Banks).

A further example concerns the deep-dive reporting requirements that are established by the Rating Agency Regulation[8], the CRR and the BRRD[9].

---

[7] OTC Derivatives Regulators Group – Barriers to Reporting Trade Repositories, August 12, 2014, http://www.esma.europa.eu/system/files/letter_to_fsb_08122014.pdf

[8] See Regulation (EU) No 462/2013 of 21 May 2013 amending Regulation (EC) No 1060/2009 on credit rating agencies; ESMA Draft Regulatory Technical Standards (RTS) under the CRA3 Regulation, Final Report of 20 June 2014 (ESMA/2014/685).

[9] See Annex 1a – Survey on Banking Secrecy Regimes in the Euro area.

Consequently, against the background of a heterogonous legal framework of different banking secrecy regimes it is far from clear to which extent reporting obligations can set aside the constraints for information transfer.

Further Practical implications for cross border acting Banking Groups

The diversity of local banking secrecy regimes negatively affects as well the fight against anti-money laundering. For instance a cross border transfer of data and information (for sharing suspicion notices) within a financial group is - at least - difficult under the German anti-money laundering act (§ 12 GWG) and likely unlawful. A prior KYC process imposes an undue burden on local legal entities of the same international banking group as secrecy laws prevent the sharing of client information for such purposes. Hence information must be collected by each legal entity for the very same client.

The majority of the financial institutions in Europe are part of an international banking group. Banking institutions with branches and subsidiaries are generally organised to manage their business as a group (i.e. a parent establishes internal policies that the other entities of the group must implement). In a centralised system information and know-how of a parent are submitted to branches and subsidiaries so that economies of scale can be achieved – also in the interest of a given cross border acting client group.

Accordingly, the sharing of client confidential information forms an important part of the ordinary course of business of this group. The privacy constraints imposed by the several national banking secrecy laws will therefore not only create legal constraints for the risk management of a group but also for its normal day to day business/functioning.

Another negative practical effect caused by local banking secrecy regulation constraints following from the above is the cumbersome set-up of a Global Customer Relationship Management tool ("CRM"). The idea of such a CRM tool is in general to facilitate the risk assessment at a global consolidated level by establishing risk/return parameters related to a client´s KPIs, RWA, P/L and other factors. Some local banking secrecy regimes prevent the sharing across legal entities unless client consent[10] can be provided for, whereas others allow a sharing of such information at least within a financial group[11].

Conclusions

The EFMLG would appreciate if the Commission could start investigating the issues raised above and may consider the following remedies and actions as it is clear that further efforts are needed at EU level so that banking secrecy can be interpreted within the EU in a uniform way.

[10] See Annex 1a and b; Client Consent is difficult to obtain and to manage: in some jurisdictions it cannot be embedded in GBT, but must be in writing and explicit (See Austria - § 38 BWG) – it must be precise and transparent enough (e.g. Germany) and it does not work between financial institutions themselves as it is not customary in the market.

[11] Spain and - under limited circumstances - Austria ("Kreditverbund").

There should be clear exemptions for prudential reporting obligations (and also for credit risk hedging and outsourcing) from national banking secrecy regimes, both at European and national law level (considering also non-European legislation as the case may be).

In order to enable a truly group-wide risk management for G-SIBs and a consistent and efficient AML system, local banking secrecy regimes should be harmonised with the aim to provide for a concept of intra-group privilege for cross-border / cross legal entity information exchange.

The EFMLG is aware that, according to recent news, political agreement has been reached, at a European level, on ending banking secrecy rules as of 2017. Nevertheless, in the wait of the possible developments, an intervention seems necessary to avoid or limit the concerns above described.

Sincerely yours,

[signed]

Dr. Holger Hartenfels
The Vice Chairman

Annex 1a

SURVEY ON BANKING SECRECY REGIMES IN THE EURO AREA

	What is the regime for banking secrecy (short description)?
AT	Pursuant to Art. 38(1) of the Banking Act, credit institutions, their members, members of their governing bodies, their employees as well as any other persons acting on behalf of credit institutions must not divulge or exploit secrets which are revealed or made accessible to them exclusively on the basis of business relations with customers, or on the basis of Art. 75(3) of the Banking Act. This provision benefits from special protection as it has been enacted as a constitutional law provision.
BE	Under Belgian law, credit institutions are bound by a *duty of confidentiality*, the breach of which may give rise to damages. It is distinct from the duty of professional secrecy (secret professionnel; Article 458 of the Criminal Code) whose breach may lead to criminal sanctions but which does not apply to credit institutions. The bankers' duty of confidentiality is not laid down in statutory law, but follows from various legal sources, in particular the confidentiality obligations arising out of the contractual relationship with the client. This duty is unanimously recognised by legal doctrine, and is usually explicitly referred to in the general terms of contract of the Belgian credit institutions. It covers all data and information that came to the knowledge of the bank in the context of the contractual relationship. It also applies vis à vis tax authorities although the latter have certain means to constrain a credit institution to provide clients data under certain conditions (essentially when there are indications of tax fraud).
CY	Under Cyprus law, any director, chief executive, manager, officer, employee or agent of a credit institution or any other person who has by any means access to the records of a credit institution is bound by banking secrecy (section 29 of the Business of Credit Institutions Laws of 1997 to (No.4) of 2013) ("the Laws"). The duty to maintain banking secrecy does not apply, inter alia, in case the customer gives his written consent, the customer is declared bankrupt or, in case the customer is a legal person, the company is wound up, civil proceedings are instituted between the credit institution and the customer or his guarantor relating to the customer's account, the information is given to the police under the provisions of any law or to a public officer who is duly authorised under that law to obtain that information or to a court in the investigation or prosecution of a criminal offence under any such law, the information is required to assess the creditworthiness of a customer in connection with or relating to a bona fide commercial transaction or a prospective commercial transaction so long as the information required is of a general nature and in no way related to the details of a customer's account; or the information is supplied for the purpose of maintaining and operating the Central Information Register set up under the provisions of the Laws or the provision of the information is necessary for reasons of public interest or for the protection of the interests of the credit institution. It should also be mentioned that, pursuant to section 28A of the Laws, all persons who carry out or have carried out a task on behalf of the Central Bank of Cyprus and the auditors or experts commissioned by the Central Bank, are subject to professional secrecy.
DE	Legal foundations: As opposed to other countries there is no explicit legal provision. Banking secrecy (BS) is however acknowledged by the courts as a part of customary law (Gewohnheitsrecht) and part of the general terms and conditions of banks offering deposits. BS is also considered an outflow of constitutional rights (re customers: informational self-determination, re banks: freedom of pursue of professional activity). Data protection law is of secondary applicability (i.e. back-up function). The Tax Code (Sec. 30a Abgabenordnung) foresees that tax authorities shall not obtain financial information on customers for general supervision. Scope: BS is defined as the obligation of secrecy of banks regarding the financial situation of their customers towards third parties. Only in cases expressly stipulated by law, information on the financial situation of a customer can be shared with public institutions. This is the case for tax authorities: They can require data from credit institutions if an investigation at the taxpayer was not fruitful. In criminal procedure BS does not apply, in civil procedure to limited extent.
EL	Any bank which enters into transactions with an individual is obliged not to share any piece of information which it came to know as a result of this contact (general banking secrecy, based on general civil law principles and deriving from the concept of professional secrecy). It is also obliged

	not to share any information regarding the deposits of its customers (art. 1§1 Legislative Decree 1059/1971 on the specific secrecy of bank deposits). The provisions establishing both aspects of banking secrecy are considered *jus cogens* and a breach can result in civil and criminal liability. Banking secrecy can in principle be lifted on the basis of a judicial decision, a specific legal provision which establishes an exemption, usually for the benefit of an authority acting in the public interest, or, in case of general banking secrecy, if the individual concerned has given prior authorisation. Banking secrecy is lifted and cannot be invoked against a request by the Authorities as follows: - Banking Supervision Authorities, i.e. Bank of Greece and competent authorities of Member States or persons authorized by them are not bound by banking secrecy for the performance of their supervisory tasks (art. 53.7 of Law 4261/2014 on the activity and prudential supervision of Credit Institutions); - Tax Authorities are not bound by banking secrecy, as they have the power to inspect and obtain information on banking transactions and assets of an individual without prior notice and consent of the concerned individual or the Hellenic Data Protection Authority; - Judicial authorities investigating money laundering and related criminal activities, the Authority for Public Investments, the Body of Inspectors of Public Administration, are not bound by banking secrecy for the purpose of obtaining information in order to perform their specific tasks; In addition, judicial authorities implementing civil law provisions for the protection of creditors (including family members) can under circumstances issue a decision ordering the disclosure of deposits up to the amount due by the depositor for the satisfaction of the claim.
ES	The principle of banking secrecy is established in Article 83 of Law 10/2014 on the organisation, supervision and solvency of credit institutions. Pursuant to this provision credit institutions and related entities should maintain the confidentiality of information relating to account balances, positions, transactions and other customer operations without communication or disclosing such information to third persons. This duty applies to information in respect of both natural and legal persons. Exception to this principle (Article 83.2 and 83.3): - Where the customer or the law permits the communication or disclosure of such information to third persons - Where the relevant information is requested by or it must be sent to the respective supervision authorities - Where the relevant information should be disclosure to comply with Law 10/2010 Law on the Prevention and Fight against Money Laundering and Terrorist Financing - Where the exchange of information takes place between credit institutions belonging to the same consolidated group Article 83 is without prejudice of the regulation on data protection for natural persons (Royal Decree 1720/2007). This means that any disclosure should be done in accordance with the data protection rules established in the Royal Decree and the recipients of such disclosure should not be able to identify the individuals to whom the data relate (unless individuals have given their consent).
ET	The term “banking secrecy” and main exceptions thereto have been explained at the Credit Institutions Act, section 88: (1) All data and assessments which are known to a credit institution concerning a client of the credit institution or other credit institution are deemed to be information subject to banking secrecy. (2) The following data are not deemed to be information subject to banking secrecy: 1) data which are public or available from other sources to persons with a legitimate interest; 2) consolidated data or other similar data on the basis of which data relating to a single client or the identities of persons included in the set of persons referred to in the consolidated data cannot be ascertained; 3) a list of the founders and shareholders or members of a credit institution and data relating to the sizes of their holdings in the share capital of the credit institution, regardless of whether or not they are clients of the credit institution. 4) information on the accuracy of the performance of obligations by a client to a credit institution.

FI	In Finnish law the provisions on banking secrecy are in Section 141 of the Act on Credit Institutions. Employees, agents and members/deputy members of the decision-making bodies of the bank and other undertakings belonging to the same consolidation group or operating on behalf of the bank are subject to the secrecy obligation. The secrecy obligation covers information on the financial position or private personal circumstances of a customer or of another person connected with the bank's activities. It also covers trade or business secrets. Information subject to banking secrecy shall be kept confidential unless the person in whose benefit the secrecy obligation has been provided for consents to its disclosure. Some exceptions to the main rule exist such as the requirement to provide information to a prosecuting and pre-trial investigation authority for the investigation of a crime as well as to another authority entitled to this information under the law.
FR	In France, Banking secrecy entails both criminal and civil penalties. Governed by article L. 511-33 of the French Monetary and Financial Code (FMFC), banking secrecy protects the clientele from the dissemination of information collected by banks. As banking secrecy is designed to protect clients' privacy, it only concerns confidential information (i.e. only precise information/figures about the situation of a specific client's account), but not general information (e.g. commercial information). Therefore, banking secrecy can be waived either by the client or under legal exemptions.
IE	The statutory provisions relevant to confidentiality, and indeed disclosure obligations, primarily stem from section 33AK of the Central Bank Act 1942 (the Act). Section 33AK of the Act does not provide that all information concerning the business of a person or body, which the Central Bank receives in the course of its functions, is confidential. Instead, it provides that where such information is confidential, then the Central Bank shall treat that information pursuant to section 33AK of the Act. Section 33AK of the Act derives primarily from the obligations of '*professional secrecy*' that arise as a result of certain EU law obligations contained within the Union Directives (in this context CRD). Section 33AK(1) of the Act provides that where a Union law (such as the CRD IV) prohibits the disclosure of confidential information gathered or acquired in the course of the Central Bank's functions as a supervisory authority in Union law (such as the CRD IV), then that obligation of professional secrecy shall apply to all members, officers, consultants and employees of the Central Bank. In circumstances where professional secrecy attaches to confidential information in the possession of the Central Bank, then the disclosure of such confidential information is prohibited unless a gateway can be identified under Union law (such as the CRD IV). In this respect it is vital to note that section 33AK(8) of the Act provides that a breach of the obligation of professional secrecy in Union law is a criminal offence.
IT	The legal protection of banking secrecy is quite weak in Italy, when compared to other legal systems: a. The concept of banking secrecy is not enshrined in any legislative provision; b. According to part of the doctrine, the concept can be derived from Article 7 of the Banking Law, whereby the staff of the Banca d'Italia can only disclose the information acquired in the context of supervisory tasks within the Banca d'Italia: under this meaning, the concept of "banking secrecy" however regards only the Banca d'Italia; c. According to part of the doctrine, the concept of banking secrecy for banks derives from civil code obligations regarding good faith (Article 1175, 1337, 1375) in contractual relationships (in case of breach of such obligation banks would be held liable for damages); d. A judgement of the Court of Cassation in 1974 (No. 2147) qualified the practice followed by banks (not to disclose customers' information) as the basis of banking secrecy for banks: these practices are considered under Italian law as a (the lowest) source of law; A judgement of the Constitutional Court in 1992 (No. 51) went further and specified that whereas a banking secrecy obligation exist for banks, against this there is no corresponding subjective right deriving from the constitution for banks customers: such obligation is instrumental to the security of trade, thus the legislator is free to narrow down the scope of this obligation in order to grant the application of other principles in the constitution. In the case at hand the Court made reference to concepts such as the general duty to contribute to the general budget with taxation (hence the possibility to limit banking secrecy obligation for the benefit of the tax administration) and to the duty for the judiciary to investigate on crimes. The Court did not mention the protection of savings (article 47 of the Constitution), which is considered the legal basis for supervision, but the same considerations may apply to supervision mutatis mutandis.

LU	Professional secrecy is governed in general by Article 458 of the Luxembourg Criminal Code, while the Grand-Ducal Regulation of 24 March 1989 specifically addresses banking secrecy in tax matters and restrict the scope of application of the right of investigation of fiscal authorities. In addition, Article 41 of the law of 5 April 1993 on the financial sector and the Law of 2 August 2002 complete the Luxembourg banking secrecy regime for what protection of individuals with regard to the processing of personal data is concerned. As it is known, the regime resulting from the combination of these provision is particularly strict: a. Banking secrecy covers **all data**; b. It protects data of **both residents and non-residents**; c. It can be opposed to **both national and foreign fiscal authorities**; d. Its violation constitutes a **criminal offence** which can be punished with up to 6 months imprisonment and a fine between 500 and 5.000 euro Nonetheless, please note that this regime will be subject to some changes in light of the implementation of **Council Directive 2011/16/EU on the administrative cooperation in the field of taxation**. Already in 2013, Luxembourg introduced in its domestic legislation rules on the exchange of information upon request, on spontaneous exchange of information and on certain forms of administrative cooperation. Most importantly, with Bill n. 6632 of 13 March 2014, Luxembourg introduced mandatory and automatic exchange of information related to employment income, directors' fees and pensions.
LV	The banking secrecy regime in Latvia is governed by the Credit Institution Law. In particular, information regarding a client and his or her transactions, which the credit institution acquires in providing financial services in accordance with an entered into contract, is non-disclosable information, which can provided to such persons themselves (for legal persons - to their authorised representatives and to their highest institutions) and to their lawful representatives. Also information regarding a credit institution and its clients, information regarding the activities of credit institution and of its clients, which has not been previously published according the procedures specified by the law, or the disclosure of which has not been determined by other laws, or which has not been approved by the council of the Financial and Capital Market Commission (supervisory authority in Latvia), shall be deemed to be restricted access information and shall not be disclosed to third parties other than by way of overviews or compilations such that it is not possible to identify a concrete credit institution or the client. Non-disclosable information can be provided to state institutions in accordance with the procedures specified in Credit Institution Law, among them – to the Financial and Capital Market Commission – for performing of the supervisory function specified by the law.
MT	The banking secrecy regime in Malta is mainly covered by article 19(5) of the Banking Act which states that all statements and other information furnished by any credit institution to the competent authority (MFSA) and the Central Bank shall be regarded as secret and confidential except as between that credit institution and the competent authority (MFSA) or the Central Bank as the case may be save that the competent authority shall furnish such information as may be required by the Minister or the Central Bank and shall inform the Minister and the Central Bank if at any time in its opinion there is concern regarding the state of affairs of that credit institution. Important is also to note that Article 34 (2) of the Banking Act provides that no person, including past and present officers or agents of a bank, shall disclose any information relating to the affairs of a bank or of a customer of a bank which he has acquired in the performance of his duties or the exercise of his functions under the Banking Act and any regulations or Banking Rules made thereunder except - a. when authorised to do so under any of the provisions of the Banking Act and any regulations or Banking Rules made thereunder; or b. for the purpose of the performance of his duties or the exercise of his functions; c. when lawfully required to do so by any court or under a provision of any law; d. for the purpose of enabling the Bank or the competent authority, as the case may be, to satisfy their respective obligations arising under Malta's international commitments; or e. when the customer expressly consents, in writing, to the disclosure of information relating to his affairs, to the extent authorised by the customer.

NL	There is no banking secrecy in the Netherlands. Confidentiality of clients' information is provided for under data protection law, but there's nothing specific for banks. Other than data protection issues, I do not see how Dutch law could provide for an obstacle for exchange of information within the SSM.
PT	The obligation of professional secrecy is established by Article 78 of the Portuguese Legal Framework of Credit Institutions and Financial Companies. Members of the management or auditing boards of credit institutions, employees, representatives, agents and other persons providing services to them on a temporary or permanent basis shall not divulge or use information on facts or data regarding the activity of the institution or its relations with clients which come to their knowledge solely as a result of the performance of their duties or the provision of their services. The names of clients, deposit accounts and their movements as well as other bank operations are in particular subject to professional secrecy. As an exception (see Article 79 of the Portuguese Legal Framework of Credit Institutions and Financial Companies), facts and data subject to secrecy may be disclosed: 1) Upon the client's authorisation, transmitted to the institution; 2) To Banco de Portugal, within the scope of its duties; 3) To the Securities Market Commission, within the scope of its duties; 4) To the Deposit Guarantee Fund and to the Investor Compensation Scheme, within the scope of their duties; 5) Under the terms laid down in the criminal law and in the law of penal procedure; 6) To the tax authorities, within the scope of its duties; 7) When any other legal provision expressly limits the obligation of professional secrecy. Besides this and as stated in Article 81 of the Portuguese Legal Framework of Credit Institutions and Financial Companies, Banco de Portugal may exchange information with other authorities such as the Securities Market Commission, the Portuguese Insurance Institute, authorities, organisations, and persons performing functions, which are equivalent to those of these bodies in other EC Member States, as well as with the following bodies belonging to a Member State of the European Community: a) Bodies which administer deposit-guarantee or investor protection schemes, as regards the information necessary to the exercise of their functions; b) Bodies involved in the liquidation of credit institutions, financial companies, financial institutions and authorities responsible for the supervision of these bodies; c) Persons responsible for carrying out statutory audits of the accounts of credit institutions, financial companies, insurance undertakings, financial institutions and authorities responsible for the supervision of these persons; d) Supervisory authorities of EU Member States, regarding the information prescribed in Community Directives applicable to credit institutions and financial companies; e) Within the scope of cooperation agreements concluded by Banco de Portugal, on a reciprocity basis, supervisory authorities of non-EC Member States, regarding the information required for both non-consolidated or consolidated supervision of credit institutions having their head office in Portugal and of their equivalent bodies having their head office in those Member States; f) Central banks and other bodies with a similar function, in their capacity as monetary authorities, and other authorities responsible for overseeing payment systems.
SI	In accordance with A214 of the Banking Act, the bank must treat as confidential and protect all information, facts and circumstances about individual clients notwithstanding the manner in which this information has been obtained. Members of the bank's governing bodies, shareholders, employees or other persons who have access to the confidential information referred to in A214 of this Act in connection with their work at the bank or provision of services for the bank, may not disclose this information to third parties or use them by themselves or enable third parties to use them. In addition The Bank of Slovenia's employees, auditors and other professionals who have acted under the authority of the Bank of Slovenia must safeguard all information obtained during the performance of supervision and other transactions for the Bank of Slovenia as confidential (A228 of the Banking Act).
SK	<u>Regime for banking secrecy (credit institutions)</u> According to Slovak legislation banks shall keep information, that is subject to bank secrecy,

	confidential and protect it against disclosure, misuse, damage, destruction, loss or theft. Subject to bank secrecy shall be all information and documents on matters concerning the clients of banks, especially information and documents concerning transactions, account and deposit balances which are not publicly available. In general such information may be disclosed by a bank to a third person only with the prior written consent of the client. There are some exceptions from this rule. Banks shall be entitled, without prior consent of the client, to provide information that is protected under bank secrecy to persons and bodies which are required by law. Without the client's consent a bank shall submit such information to the National Bank of Slovakia, persons commissioned to exercise supervision, auditors and to other persons stated by law. On the basis of written request and under the conditions stated by law a bank shall submit, without the client's consent, to public bodies/authorities such as e.g. a court, a law enforcement for the purposes of criminal prosecution, a tax authority, a court executor assigned to conduct execution proceedings. Providing information that is subject to bank secrecy abroad must be in line with conditions of Act on personal data protection or international treaty binding upon the Slovak Republic. **Regime for banking secrecy from the side of the National Bank of Slovakia** In relation to banking operations of the National Bank of Slovakia and its clients banking secrecy shall apply. Information submitted by a bank to the National Bank of Slovakia and protected under bank secrecy shall be treated as confidential. All employees of the National Bank of Slovakia shall be obliged to observe confidentiality with regard to matters of their office (professional secrecy).

Annex 1b

SURVEY ON NATIONALSECRECY RULES, DATA TRANSFER REQUIREMENTS AND APPLICABLE SANCTIONS IN THE EURO AREA

The guiding questions of the below survey are:

1. What are the Banking Secrecy Rules in your country (Legal Source, scope – data types)
2. How does these rules deal with / interact with data transfer for Risk Management Consolidation , KYC, Foreign Authority Requests, and Intra Group business steering purposes?
3. Is a client consent for data transfer required in these cases and if so are there any formalities?
4. What are the sanctions associated with a breach of banking secrecy and are there any pre-requisites?

Definitions/Types of data considered:

1. Biographic data: e.g. customer's name, registered office address, correspondence address, legal form (ltd etc.), fiscal code, registration code etc.
2. Risk data: e.g. credit analysis, rating, financial position, granted lines, utilized balances, provided collateral etc.
3. Commercial data: e.g. Client Service Team composition, profitability by product, volumes, RWA, profit planning, competitive environment, market strategies
4. If not specified otherwise in the respective field or column
   a. "Data Transfer Intra-Group" means a transfer of data among credit institutions controlled by a parent institution (including such parent institution)
   b. "Authorities" means any local or foreign authority which is a (i) public authority or body officially recognised by national law, which is empowered by national law to supervise institutions as part of the supervisory system in operation, or (ii) a public authority which is empowered as tax, criminal, or administrative body including courts or other judicial bodies

Country	SECRECY RULES [under the condition that data do not refer to physical persons]	DATA TRANSFER Intra-group	to Authorities	to Other 3rd Parties	REQUIREMENTS FOR DATA TRANSFER	SANCTIONS (w/o Reputational Risk)	PREREQUISITES FOR APPLYING SANCTIONS
Austria	BIO DATA Disclosable in specific cases (among which "overriding legitimate interests pursued by the controller") RISK DATA Banking secrecy (Sec. 38 BWG) COMMERCIAL DATA Banking secrecy (Sec. 38 BWG)	for Risk Management & Consolidation purposes a. up-stream b. intra group Sec. 30 (7) BWG for Intra-Group business steering purposes: KYC Sec. 40 BWG			The client's explicit consent is required Exemptions are for Risk Management Purposes Foreign Authorities	ADMINISTRATIVE - fines up to €. 19,000 and 30,000 for, respectively, violations of data protection and banking secrecy provisions; - other measures possible under Banking Act (the most serious being the revocation of the banking license) **CRIMINAL** **- imprisonment up to 1 year**	CIVIL sanction: proving the damage/distress suffered

						CIVIL - compensation for damages	
Belgium	Belgian bank secrecy rules were not embodied in a statutory provision. Note however that there are different legal sources on which the bank secrecy rules may be based, in particular the confidentiality obligations arising out of the contractual relationship between a financial institution and its client in relation to the banking business carried out for the client. Additional legal sources include amongst others customary law (this duty was created to a large extent by the legal doctrine). Note that the application of the banker's duty of confidentiality is often explicitly confirmed in the general terms of contract of the Belgian financial institutions. All data shall be subject to the banker's duty of confidentiality.				Data transfer of all data is prohibited unless (i) a prior written consent of the counterparty is obtained; (ii) if disclosure is required or authorized by or under law or if (iii) if the bank's own interests require such disclosure.	Criminal: A breach of a duty of confidentiality does not constitute a criminal offence <u>unless</u> if there is a breach of the Belgian personal data protection acts at the same time. CIVIL: compensation for damages	Client may claim damages for breach of contract (art. 1145 of the Civil Code). However if evidence of an agreement cannot be shown, article 1382 of the Civil Code will come into play (here, client will have to prove that there has been a fault, damage and a causal link between the two).

Germany	BIO DATA Banking secrecy (already existence or non existence of a banking relationship is covered; only public register data disclosable); RISK DATA Banking Secrecy COMMERCIAL DATA Banking secrecy (unless publicly available)	for Risk Management & Consolidation purposes a. up-stream b. intra group for Intra-Group business steering purposes: not possible KYC: GeldwäscheG ; no intra-group information sharing			The client's consent is required but per Special Business Terms possible Within the constraints of § 44a KWG Article 11 (1) CRR up-stream flow is possible.	ADMINISTRATIVE - by repeated banking secrecy breaching, BAFIN orders measures to be taken to reduce the risk (high reputational risk); if the Board does not comply, BAFIN may revoke Board members or finally cancel the banking license. **CRIMINAL** - **none for banking secrecy** CIVIL - compensation for damages - right to terminate customer relationship	BaFin may investigate on its own initiative or based on customer complaints and will impose a sanction if "findings" individual: proving the damage/distress suffered
Portugal	General consideration concerning bio data: Data protection rules are not applicable to legal entities, including when relating to individuals such as corporate representatives, when such information is made available to the public (i.e. public registries) or directly provided by the client. However, depending on the purposes of the processing of such information, data protection rules may be applicable in relation to such representatives (consent from data	General consideration concerning bio data: Data protection rules are not applicable to legal entities, including when relating to individuals such as corporate representatives, when such information is made available to the public (i.e. public registries) or directly provided by the client. However, depending on the purposes of the	ALL DATA: Facts and elements covered by the secrecy duty may be transferred to the Bank of Portugal, the Portuguese Securities Commission, the Deposit Guarantee Fund, the Investors	The client's explicit consent is required.	The client's explicit consent is required. Exemptions mentioned in the previous columns.	ADMINISTRATIVE **Breach of data protection rules:** - Fines that may range between EUR 1,500.00 and EUR 15,000.00. **Breach of banking secrecy rules**: - Pursuant to the RGICSF, if a credit institution breaches the banking secrecy rules it is bound to, it is considered to be committing an administrative offence (*contraordenação*), entailing a fine ranging from EUR 3,000.00 to EUR 1,500,000.00. Furthermore, under the RGICSF, an administrative	CIVIL sanction: proving the damage/distress suffered BdP may investigate on its own initiative or based on customer complaints and may impose sanctions and other measures to stop the breach of secrecy duties – article 76 and 116 RGIC The Data Protection Authority may also

	subject and/or notification duties at the Data Protection Authority) (e.g. marketing, money laundering, accounting purposes etc). ALL DATA is covered by banking secrecy, established by Article 78 of the Portuguese Credit Institutions and Financial Companies Legal Framework ("**RGICSF**"), *i.e.*, may not be disclosed without the client's authorisation	processing of such information, data protection rules may be applicable in relation to such representatives (consent from data subject and/or notification duties at the Data Protection Authority) (e.g. marketing, money laundering, accounting purposes etc). ALL DATA is covered by banking secrecy, established by Article 78 of the Portuguese Credit Institutions and Financial Companies Legal Framework ("**RGICSF**"), *i.e.*, may not be disclosed without the client's authorisation	Compensation System and the judicial and tax authorities in accordance with the applicable law.			offence (*contraordenação*) may lead to the imposition of ancillary penalties, such as the apprehension and loss of the object of the infringement, including its proceeds, and the release to the public of the final punishment by the BdP, at the expense of the defaulting party. CRIMINAL - Imprisonment up to 1 year for violation of the banking secrecy. - imprisonment up to 1 year or fine up to 120 days for unauthorized access do private data CIVIL - compensation for damages	investigate on its own initiate based on a complaint and may impose sanctions – articles 23 and 38 of the Data Protection Act

Spain	BIO DATA Disclosable pursuant to article 2.2. RD 1720/2007 (provided it does not make reference to individuals). RISK DATA Banking secrecy, unless publicly available (first additional provision of Law 26/1988). COMMERCIAL DATA Banking secrecy, unless publicly available (first additional provision of Law 26/1988).	With respect to credit institutions belonging to the same consolidated group (including affiliates of foreign jurisdictions).	Supervisory competent authorities when requested or pursuant to applicable law.	If disclosure is authorized by the Client or is made pursuant to applicable law.	- Client's explicit consent. - Applicable law. - Supervisory competent authorities. - Intra-group data transfer.	ADMINISTRATIVE Infringements of the bank secrecy regulation constitutes a "serious offence", implying monetary sanctions (maximum amount of 500.000 euros or 0,5% of the bank's shareholder equity) or other administrative measure (the notification obligation of the infringement in the official gazette). CRIMINAL Imprisonment up to 5 years. May be associated to monetary sanctions and disqualification from the exercise of the profession. CIVIL Client may seek compensation before the appropriate courts.	For administrative sanctions, the Bank of Spain is the competent body to carry out the administrative proceeding and impose the corresponding sanction.
Italy	BIO, RISK, COMMERCIAL DATA Banking Secrecy (principal rules, no laws) Data Protection legal entities removed from the Italian Privacy Code (196/2003) as per December 2011(i.e. a bank is enabled to share the data related to its corporate customers (legal entities) within its banking group)				no consent needed for the legal entities related data transfer (if the purpose is <u>not</u> marketing)	CIVIL the bank is liable in case of causing a damage to the customer	proving the damage suffered

France	ALL THE DATA Banking secrecy (French Monetary and Financial Code)	for Risk Management & Consolidation purposes a. up-stream b. intra group c. KYC for Intra-Group business steering purposes			Financial institutions may disclose confidential information to entities belonging to the same group i) with an explicit consent of the client ii) on a case by case basis ("need to know basis") where any type of contract or transaction is under consideration or is being worked on	ADMINISTRATIVE fine up to EUR 15,000 **CRIMINAL** **- 1 year imprisonment**	
UK					implicit consent possible via GBTs	not every breach of the UK's Data Protection Act is an offence ADMINISTRATIVE in case of individuals suffering damage, a financial penalty may be imposed by the Information Commissioner (the Information Commissioner's Office is the UK's independent authority set up to uphold data privacy for individuals, the most common) **CRIMINAL** **none** CIVIL claim for damage / distress compensation from individuals	- Authority: a claim - individual: proving the damage/distress suffered

LUX	ALL THE DATA Banking secrecy (Law on the financial sector)				Data sharing to third parties is a criminal offence and as such may not be waived (not even an explicit customer's consent is valid) Questionable whether professional secrecy may be waived by client's consent (no court ruling decision so far) In any case, if client's consent is viable, the following criteria must be met: i) it must be in person's interest ii) clause must be specific in terms of precise information, recipients, purpose and time	ADMINISTRATIVE fine EUR 500 – 5,000 **CRIMINAL** **imprisonment for up to 6 months** (upon the directors of the company)	the fact of committing the offence
US	BIO DATA disclosable RISK DATA Banking Secrecy COMMERCIAL DATA Banking Secrecy				US has no comprehensive data protection legislation of the sort that exists in Europe with respect to B2B relationships. US does not impose any legal limitations relevant to the transfer of company data from one UniCredit LE to another	ADMINISTRATIVE none* **CRIMINAL** **none*** CIVIL SANCTIONS information sharing without client`s consent / violation of a non-disclosure agreement which causes monetary damages entitles for a suit to recover the damages (*to be confirmed)	only measurable monetary damage caused by exchange of information may entitle to file for a suit