



**Department of Policy and Business Practices**

# **ICC-Fact Finding Questionnaire Basel II and Data Protection**

## **Questionnaire and Answers**

prepared by Rainer Knyrim, Preslmayr Attorneys at Law, Vienna

### I. Introduction

1. Basel II requires banks to collect and exchange huge amounts of data, including customer data falling under data protection legislation. It is surprising to read that with respect to the difficult relationship between data protection and Basel II, the draft of the new EU capital requirement framework (EU Council Doc Nr. 12890/05 – “New Directive”) has just one paragraph in its introduction reminding credit institutions that *they* “will have to adjust their data processing needs to their clients’ legitimate data protection interests as governed by the existing Community legislation on data protection”. In other words, the New Directive will lay the problem into the hands of the banks and will not solve it itself. References to data collection in the New Directive have an extremely general wording which do not give any idea which kinds of data banks will *really* be allowed to process and *in what way* they will be allowed to share it internally or externally (example: Art 84 2 (d): “The credit institution collects and stores all relevant data to provide effective support to its credit risk measurement and management process.”).
2. The draft of the New Directive already requests banks to collect data now. This data is needed to do the requested ratings in the future (example: Art 154 5. and 6. New Directive requiring banks to have two years of historical data at the End of 2007). It is questionable how banks shall fulfill data collection duties now which are laid down in a (draft) directive which has not been transposed into national law.
3. The rating provisions request the collection of huge amounts of data on their bank customers and banks already collect customer data of various kinds, including for example soft facts (like private/family issues of company managers). Banks question whether they really have the right to collect and process this data which comes from many different sources and is collected partly without the customers knowledge. The draft of the new directive does not give any useful help in solving this question.
4. To do ratings and settle credit limits on large customers which are clients in different banks of a banking group, data needs to be exchanged both EU-wide as well as globally which leads to the well-known data transfer problems. Experience has shown that the argument of a prevailing interest of the bank is more difficult to argue in discussions with data protection authorities than was thought and international and national laws were not precise enough to serve as a legal basis for a transfer.



The draft of the New Directive may be downloaded at:

[http://europa.eu.int/comm/internal\\_market/bank/regcapital/index\\_en.htm#capitalrequire](http://europa.eu.int/comm/internal_market/bank/regcapital/index_en.htm#capitalrequire)



## II. Questionnaire

In a first telephone conference on February 22, 2006, participants raised various questions on the subject and some key issues were discussed. To find out more facts on problems of banks in the field of Basel II and data protection, ICC sent out the following questions. Below please find the questions and the answers received by the ICC from banks. Bank names have been anonymized.

### **1. Will Basel II cause changes in the way (intensity, depth etc) you collect and process rating data?**

Yes, we confirm that Basel II will cause significant changes in the way rating data are collected and processed by H. Bank.

The Capital Adequacy Directive will cause some changes in the way that Bank C. will collect and process rating data.

Yes. Banks will be required to broaden their current data base and collect data at a much more granular level than at present.

Yes.

No.

Yes, it will.

### **2. Does your bank already collect rating data on its customers to fulfill Basel II requirements? Is your bank already collecting or will it collect “soft facts” on its customers? Will it collect sensitive data like race, religion, health or criminal information of key personnel of your customer? Will your bank use data on its customers received from third parties?**

The first sentence refers to rating data. It is important to explain what this word means. Credit ratings are given by various agencies to (predominantly) large institutions or organizations or to debt or other instruments issued by them. In addition, banks are required to assign customers to various internal credit grading or rating buckets.

H. Bank is planning to start collecting rating data (including sensitive data) to fulfill Basel II requirements.

Bank C. does collect a form of internal rating data on its customers. The Bank already collects data on ‘soft facts’. Sensitive data related to the race or religion of the key personnel are not collected by the Bank. However other sensitive data like health or criminal information may be of use if they come to the attention of the Bank. For the moment this is not happening but in the future the Bank may use such data on its customers received from third parties for rating purposes.



South African banks already collect data on most of their customers, however internal rating coverage is not yet complete. The banks retail portfolios are substantially complete and the corporate counterparties anticipate completion by the end of 2007. Banks collect data on most of their customers; however historic credit vetting data on unrated clients' is generally in hard copy on file, not electronic. The banks expect to have uniform approach to managing electronic rating data and collect all counterparties data in electronic format by the end of 2007 to satisfy Basel II requirements.

Banks collect data on key personnel (eg Directors/shareholders) where surety has been provided by them for the counterparty. As far as it would improve the estimation of credit risk, processes to expand data collection would be considered.

Any sensitive data collected is subject to the Constitution of South Africa and where sensitive data is collected it is permitted under specific legislation such as Employment Equity Act etc.

Bank staff that are dismissed due to criminal offences are listed on The Banking Association REDS data base for use by Human Resources managers within the Banking Industry only.

At present entities within a banking group can share counterparty data whilst external data source (Bureau Agencies eg Experian & ITC) can be purchased or acquired to enhance risk estimation. Intended Privacy Legislation will require the consent of the customer.

Yes, the bank has already collected rating data on its customers to fulfill Basel II requirements and those soft data and sensitive data may also be collected. In certain circumstances, third parties data may also be used.

No.

Yes.

X. is indeed, in the context of the gradual implementation in Sweden of the Basel II framework, collecting data on its customers from internal, as well as external sources. As regards the question on soft facts, the answer obviously is connected to how one defines this notion. If one takes the example mentioned under Introduction, section 3, X. does not today process data on company representatives' family issues. However, X. is (of course) considering to process data on company representatives regarding creditworthiness (which for us, at present, does not include family issues).

Specific legislation in Sweden (kreditupplysningslagen) regulate what information on creditworthiness credit bureaus can provide and how it should be handled. A record of non-payment of debt have to be based on a legitimate basis according to certain rules.

But what about bank-internal information on creditworthiness ? The mentioned legislation is not applicable for credit institutions. To what extent is it allowed for a bank in its credit analysis to take into account that a board member consistently is three or four days late with his mortgage payments or payments on his credit card debt (but never defaults)? Would a company accept that such data affects the rating of the companies creditworthiness and thus the pricing of products? There is also uncertainty to what extent data of this kind may be transferred between different parts of a banking group. X. for example handles its card business in a specific group of subsidiary companies. Here X. feels quite confident that data on creditworthiness connected to the X.-branded cards may be transferred to the parent bank company and processed for Basel II purposes.

However there has been a discussion if this also is OK when it comes to cards with another brand. In other words: would it be OK to transfer data on creditworthiness from



a non-X. brand subsidiary to the parent company and use it for Basel II purposes ? In such case there is, for the customer, no visible connection between the supplier of information and the receiver and subsequently customers might find such processing of data as an infringement of privacy/integrity.

No, we will not.

Yes, for example from credit bureaus and public company registers.

**3. To settle credit limits on large customers which are clients in different banks of a banking group, will your bank exchange customer/rating data within its banking group or with other banks/third parties? Will this transfer involve cross border data flow outside the EU?**

First, I would like clarification on the extent to which ‘large customers’ are affected from a ‘data protection’ point of view. Second, the process described is the standard one employed for granting credit limits and is not affected by Basel II. I wonder whether the confusion arises from the process proposed by banks and agreed with regulators for banks to be able to pool core historical credit data (generally on a national basis) so that they would have enough data to make a statistically acceptable allocation of customers into the various ratings ‘buckets’ or along the relevant rating curve. This is a very different process from granting individual credit limits. In any case, the data pooling is applied for smaller, rather than larger customers.

On the issue of whether H. Bank will exchange customer / rating data within the H. Bank group or with other banks / third parties, we note the following:

- Data is already being exchanged between the companies belonging to the H. Bank group. We note that the official notification sent to our National Data Protection Agency regarding the maintenance of an archive containing customer data, concerned a central archive for the H. Bank Group, which is kept by H. Bank. This position is also reflected in our current Customer Consent Declaration form which is entitled “Your personal data and the H. Bank Group”.
- As regards the issue of exchanging information with other banks / third parties we need to ascertain whether this is intended to take place / or indeed whether it is necessary, due to Basel II, to take place on a regular basis.

There may be some cases where the exchange of customer/ rating data within Bank C. group is taking place. For the moment no customer/ rating data is exchanged with other banks/ third parties. Moreover Bank C. has subsidiary in A. and is planning to expand to some other countries outside the European Union, so there may some cases of cross border data flow.

Within a banking group, individual banks will exchange rating data; however sharing with other banks/third parties would be subject to the arrangement between the parties. A bank may enquire with another bank for a rating of the client using an industry coding system that qualifies a client’s transaction behaviour related to risk profile. E.g.: a cheque issued in settlement of a debt could be verified by the issuing bank ie good for funds.



In South Africa no restriction exists on cross border data flow and South Africa banks will share data with their African and EU operations.

Yes, certain credit limits on large customers may be exchanged within the banking group for the purpose of control but not to third parties except the regulators. The data transfer may involve cross border data flow outside EU but is limited to the credit control units for credit limit monitoring.

No.

X. is exchanging data within the group to settle credit limits. This is done inter alia to live up to regulatory demands on the handling of large exposures for banking groups. The transfer does involve cross border data flow outside the EU since X. has branches outside the EU. At present X. is not exchanging data with other banks regarding the settling of credit limits. However X. is in the process of joining PECDC (Pan European Credit Data Consortium). PECDC is a joint venture between several European banks and Fitch Risk. The member banks which contribute with non-retail default data, get several ratios regarding LGD and EAD from Fitch risk and will also get access to the anonymous raw-data for own calculations etc. However, in the process of joining PECDC, we have pondered upon questions regarding bank-secrecy and data protection. One problem concerning bank-secrecy is that you sometimes can conclude what company anonymous data stem from. The default data in itself indirectly might lead to such a conclusion. Is this OK? The result might be that a bank participating in the data pool have broken its obligation of secrecy. Another concern in Sweden is that the mentioned legislation on the handling of data on creditworthiness not was written with the data-pooling concept (or other Basel II consequences) in mind which leads to legal uncertainty. At present this legislation is being dealt with by the Swedish Ministry of Finance.

**4. Will such credit limits be settled by using a joint data base to which different legal entities of your banking group will get access or will there be a central unit in your banking group collecting the data, forming a credit limit and distributing only the information to each entity which is relevant to it? Or will your bank establish another system?**

Credit limits will be settled by using a joint database to which the different legal entities belonging to the H. Bank Group will have access.

Each separate entity within the Bank C. Group has its own database about customer's data. Any specific information that is required by any of the entities from another entity is distributed on request, only to that entity to which it is relevant.

At present data is shared on ad-hoc request however no centralised data base exists where data is collated and shared within the group. System development will be driven by the need for enhanced credit risk estimation.

The joint data base is maintained by a central credit control unit of the banking group which will distribute the data to appropriate party in the banking group for discharging its responsibilities.

Not Applicable.



The latter. X. thus has a central unit collecting the data, distributing only the information relevant to the respective unit. The thought is that each entity should not have access to more information than necessary, which would be in conflict with principles of bank secrecy.

**5. Is your bank planning to try to solve the Basel II data protection issues by using consent declarations of its customers? If yes, would this consent declarations be used in all cases or only in specific situations (like special groups of customers or special business areas).**

As regards the issue of compliance with the Data Protection obligations arising from Basel II by using consent declarations of our customers, we note that the issue of whether or not specific consent declarations will be deemed necessary, will depend on:

- a. Whether our current national legislative provisions on data protection can be interpreted as adequately covering the issue of processing data for Basel II purposes. More specifically, it depends on whether section 5(2)(e) (among other provisions) of our national Data Protection Act (which allows for the processing of data without the need for consent by the customer in cases where “*such processing is necessary for protecting / satisfying the legitimate interests of the person processing the data*”) will be interpreted as covering the Basel II data processing requirements.
- b. Whether our current consent declarations can be considered adequate to cover the kind of data and processing required by Basel II. More specifically, our current consent declaration form states that the H. Bank Group may process customers’ data for the purpose of “*appraising economic and financial risks and for the monitoring of money laundering and fraudulent activities*”. Will this be considered sufficient?
- c. Whether Basel II will require the processing of “sensitive” data for which specific consent is necessary or whether transfer to third parties outside the H. Bank group will be necessary.

In all the cases that data protection issues are raised, the Bank intends to use the consent declarations of its customers. These consent declarations will be use only in specific situations.

Yes, banks will comply with the proposed Privacy Laws which require consent declarations of its customers.

The design of approach would depend on the requirements of each operation.

Not decided Yet.

No, X. has no thoughts at present on using consent declarations. For private individuals we believe it is very important that the regulations are as clear as possible on what data credit institutions are obliged/allowed to process. Consent declarations are not an option here ; if a certain processing of data is not allowed without consent according to the legislation on data protection we in most cases do not want to carry it out. For



companies the definition of the problem might be different, but as mentioned, we have no thoughts on using consent declarations at present.

**6. Would your bank prefer to get clear international/EU and/or national legislation? which would make consent declarations unnecessary?**

It would definitely be preferable for either EU or national legislation to make it clear that consent declarations are not necessary. It would avoid uncertainty and a great deal of cost for the banks.

The Bank prefers to get clear international/ EU and/or national legislation, which would make consent declarations unnecessary.

At present the legislation is focused towards privacy protection and blanket amnesty is not yet being considered.

Yes, clear international/EU and/or national legislation may provide assistance to bank in compliance of the requirements.

No.

Definitively (see also under 5 above).

**7. Has your bank thought on how it will treat data subject access rights like information, correction, deletion rights of it's customers concerning their data/rating data?**

The issues raised in these questions, have not yet been dealt with internally by our Bank.

The Bank will definitely introduce rights of access to different users concerning their data/ rating data. The Bank already applies that for other data.

Within the current legislative environment specific processes have been developed within the banks and with the introduction of the Privacy Protection legislation these processes will be reviewed and enhanced where necessary.

Yes, the bank has laid down procedure and guidelines for data security which governs the rights of different parties on the data access including information, correction, deletion, etc.

No.

Yes, this is an issue we have identified as somewhat problematic. On the one hand the traditional view has been that banks are not obliged to disclose detailed information on its risk measurement processes that can be regarded as business secrets. On the other hand the trend in the data protection area has been the opposite; customers have indeed the right to have detailed information on what and how his/hers data are being processed. At present X. of course try to balance these interest as conscientious as possible. However, clarifying legislation on how the customers rights of information,



correction etc should be balanced against the interests of the banks would be of great help.

**8. Has your bank already raised privacy issues and data protection issues with regard to Basel II duties internally? Has your bank designated people to work on the subject of Basel II and data protection?**

The issues raised in these questions, have not yet been dealt with internally by our Bank.

Bank C. has not raised privacy issues and data protection issues with regard to Basel II.

There is no specific initiative at present.

No, Basel II data protection is being incorporated within the existing legislative framework.

Yes, the bank is aware of such issue and will cater it in the data collection process.

No.

Yes, we have. Several issues have been and are being discussed along with the implementation of the Basel II framework.

No, we do not have people who work with this issue only. There are however people, such as myself, within the banks different divisions and units who have a special responsibility for data protection issues.

**9. Does your national legislation contain any specific provisions on Basel II and data protection or do you know about projects/drafts to do so? If yes, please indicate those or send us a copy or on online link to them.**

We are not aware of any provisions of our national legislation dealing specifically with Basel II and data protection issues.

Up to now there are no specific guidelines or rules from the national regulator regarding data protection issues for Basel II.

No specific Basel II legislation deals with data protection, however the South African Law Reform Commission has recently released Discussion Paper 109 dealing with Privacy and Data Protection.

<http://www.doj.gov.za/salrc/dpapers.htm>

Framework has already been laid down in our local legislation for the implementation of Basel II but no specific provision has been contained for the issue of data protection.

No.

No, our legislation does not at present contain any specific provisions. We face the demands in the Basel II framework on the one hand and the demands in the data protection legislation on the other. Work is being done in the Ministry of Finance, but as of yet, without no drafts or results in this area.



**10. Do you think that the current/drafted (if existing) national data protection legislation and banking legislation in your country is clear enough to make it certain to your bank how to solve data protection issues raised by Basel II?**

With regard to the issue of whether our current national data protection and banking legislations are clear enough for our Bank to understand how to deal with the Basel II data protection issues, we would state that we are rather unclear on whether data processing effected in compliance with Basel II falls within any of the established exceptions of our national Data Protection Act or our National Banking Law (e.g. “*the protection / satisfaction of the legitimate interests of the Bank*”). We would thus be inclined to seek customer consent, where possible, for e.g.

- (i) the collection of sensitive data and
- (ii) the transfer of data to third parties outside the H. Bank group, that may be necessary under the Basel II provisions.

The current national data protection legislation and banking legislation is clear enough, although there is no provision for the Basel II issues.

The existing legislation does not specifically protect privacy, however it provides for some voluntary provisions under the Electronic Communications and Transactions Act with provisions to request information under the Promotion of Access to Information Act.

The draft bill on data protection is a hybrid between the European Union directive aimed at protecting human rights and the OECD guidelines aimed at market efficiencies. The existing and planned legislation should address any issues deriving from Basel II implementation.

There are no legislation issues raised for data protection to cater for the Basel II requirement.

Yes.

As been stated under 9 above in Sweden we have a conflict between two different regulations, and no specific legal provisions helping us deal with it. Even if a lot of issues can be solved using the principle of the weighing of interests etc. there is uncertainty in some areas. This means a risk that different institutions come to different conclusions which might have impact on customers. Since the Financial Supervisory Authority is very keen on getting the best possible application by the banks of the framework on capital requirements from a economic stability perspective, there might also, to a certain extent, be a risk that credit institutions might go too far from a data protection perspective whilst striving to live up to these requirements. To sum up, our view is that Swedish legislation at present not is clear enough.

**11. Do you think that international/EU legislation currently covers the data protection issues raised by Basel II sufficiently?**

We do not believe that our current national data protection legislation sufficiently or clearly covers the Basel II data protection issues. In the face of such uncertainty, we



would obviously tend to adopt a conservative approach and try and obtain customer consent in most cases, at a significant procedural and monetary cost to the Bank.

We think that existing international/ EU legislation does not sufficiently covers the data protection issues raised by Basel II.

N/a

We think there is room for improvement on the legislation.

Yes, regarding standardised approach.

Our view is that existing regulations not sufficiently covers the data protection issues raised by Basel II.

**12. Has your Bank already addressed the privacy issues of Basel II with national Data Protection Authorities or Banking Authorities/Associations? Or do you know about any ongoing projects/discussions in this field?**

Our Bank has not addressed the privacy issues of Basel II with our National Data Protection Authority. The matter is currently being looked into by the Association of Commercial Banks.

Bank C. has not addressed the privacy issues in Basel II with the Central Bank.

Banks have not specifically raised this issue.

Not at present.

We basically follow the privacy rule.

No.

An initiative was taken by the banks through the Swedish Bankers Association in the beginning of 2003. The Swedish Data Inspection Board was contacted. The authority delivered a short decision memo in which it, amongst other things, stated that it would be very helpful if the future Basel II legislation also would deal with data protection issues.

Following this discussion, one other issue has been discussed regarding to what extent client executives should have access to detailed Basel II information whilst granting/processing credit applications. This is an example where the Swedish Financial Supervisory Authority in its draft of regulations and general guidelines concerning internal classification of risk, applies the Basel II requirements so that it comes in conflict with the above mentioned statement from the Swedish Data Inspection Board.



**13. Have you read any newspaper/legal articles/studies on the issue of Basel II and data protection? If yes, please send us a copy or online link to it as it would help us to show that the subject is a public issue. Have you heard about any conferences on the subject? If yes, please send us information on it as well.**

We have not read any articles etc on the issue of Basel II and data protection. Should we come upon such articles, we shall forward them to ICC.

No articles are seen to be available providing any information about data protection issues and Basel II.

No.

This particular issue has not been specifically raised in the local discussion of Basel II.

No.

No, I've heard of no legal articles etc or conferences regarding this specific issue. There has to my knowledge and to this point been almost no public debate on this issue.

**14. Do you think it would be useful that ICC forms a task force on this issue or a joint task force consisting of data protection and banking task forces? Would your bank like to be actively involved in such task force? Would your bank be willing to share costs occurred in such task force?**

Yes, we do believe that the creation of a task force on the issue under consideration will be useful. As far as our active involvement in such a task force is concerned, as well as the possibility of sharing any possible costs, we note that we cannot commit ourselves unless we have specific information on the terms of reference of such task force, the estimated man hours required and the estimated share of costs.

It will be very useful for ICC to create a task force on this issue, and our Bank is willing to get involve with this project. As far as the cost is concerned a cost and benefit analysis will have to be carried out in order to decide.

In the absence of existing international structures a task force would be justified. X. tends to follow international best practice.

The Banking Association is a non profit organisation and would not be in a position to contribute financially.

Considering the size of our Bank's current operation in Europe, it will not be cost effective for our Bank to actively involve in any task force on this issue at this moment.

No.

Yes, we think a task force would be useful and that it's purpose should be to develop a position on the Basel II – data protection issue. I would like to participate on behalf of X. in the work carried out by such a task force. Regarding costs X. is prepared to, within



reasonable limits and my managers approval in each case, bear the costs for my involvement, including costs for travel and accommodation. However, at this stage I cannot make a commitment regarding other costs. I would have to – in each case – discuss an issue regarding such costs internally first.

**15. Do you think that such task force should include banking secrecy questions in its work? Has your bank discussed banking secrecy issues with regard to Basel II? Have you heard about any ongoing discussions, legal articles, conferences on banking secrecy and Basel II?**

With regard to banking secrecy issues arising from the Basel II provisions, please note that although we have not yet discussed these internally, we believe that such a discussion would be useful.

Banking secrecy questions must be raised as a different issue.

Not sure what constitutes bank secrecy.

No.

This particular issue has not been specifically raised in the local discussion of Basel II.

No.

Yes we think the task force should include banking secrecy issues. In connection with the discussions mentioned above regarding data protection issues, X. has also encountered banking secrecy issues and they are often closely connected to the data protection issues. I've heard of no legal articles, conferences etc on the specific issue of banking secrecy and Basel II.

**16. Has your bank already implemented the necessary anti-money-laundering and anti-terrorism measures and solved the data protection issues linked to this subject (including, if necessary notification or approval by the local data protection authorities)? If no, do you think that the current national legislation in your country is sufficient to solve the data protection issues linked to anti money-laundering and anti terrorism measures? Do you think that ICC should get involved in this matter as well?**

As regards data protection issues arising from anti-money laundering measures, please note that our national Banking Law expressly provides for an exception to banking confidentiality where the disclosure of customer information is required “*either by law or following a Court Order*”. Our national Data Protection Legislation also provides for an exception to the obligation to obtain customer consent in the event where the processing of the customer’s data “*is necessary for the fulfillment of obligations imposed by law.*” Taking into account that there is a specific law dealing with anti-money laundering matters and procedures, we believe that this matter is sufficiently dealt with in our national legislation.

Bank C. already implemented the necessary anti-money-laundering and anti-terrorism measures.



Anti-money laundering (AML) and combating the financing of terrorism (CFT) measures are being implemented on an ongoing basis in compliance with latest international and local developments. However, as noted above, a draft data protection bill has been released for public comment, and we have noted inter alia that the bill needs to accommodate statutory AML/CFT requirements on banks and other private sector institutions.

N/a

No – this is the preserve of the OECD’s Financial Action Task Force.

We have already implemented the necessary anti-money-laundering and anti-terrorism measures according to the supervisory guidelines issued by the local regulator. Yes, our Bank has already implemented anti-money laundering, anti-terrorism measures. We do not think that ICC should get involved in this matter.

X. believes that this task force should not get involved in the matter of AML and CFT. The main reason being that this would make the scope of the task force too wide to handle. Regarding AML/CFT and generally speaking, X. is in the process of reviewing routines and procedures as a consequence of the FATF:s evaluation of Sweden and the upcoming third EU-directive on AML and CFT. There are in this context several issues that can be raised regarding data protection, but as mentioned, we feel this should be out of scope for this task force.