Project co-funded by the
CIVIL JUSTICE PROGRAMME
of the EUROPEAN UNION

iSupport
cross-border recovery
of maintenance obligations
*pour le recouvrement*
*transfrontière des*
*obligations alimentaires*

**iSupport Data Protection Working Group (4) - 15 January 2015 Meeting**

# Draft Report of Meeting n°1

**List of Participants**

| **Experts** | **iSupport Team** |
|---|---|
| Bert BLÖS (Estonia)<br>Robert BLUKIS (Latvia)<br>Mary BUTLER (United States of America)<br>Simone CUOMO (CCBE)<br>Inez LOPES (Brazil)<br>Hannah ROOTS (NCSEA)<br>Eduardo SPANO JUNQUEIRA DE PAIVA (Brazil)<br>Thomas STEIMER (Switzerland) | Philippe LORTIE (Chair)<br>Brigitte VOERMAN<br>Juliane HIRSCH<br>Marie VAUTRAVERS<br>Patrick GINGRAS |

## I. OPENING OF THE MEETING

### Introduction

1. Philippe Lortie, First Secretary, welcomed all experts to the Meeting of the Data Protection Working Group.

2. Philippe Lortie explained the role of the Data Protection Working Group which is to discuss and address data protection issues from a technical and legal perspective in the context of the development of the iSupport electronic case management and secure communication system. Philippe Lortie announced the launch of an iSupport specialised section on the Hague Conference website where the necessary documentation and the meeting reports will be available.

## II. DATA PROTECTION RELATED ISSUES

### Database and application in the cloud v. Local implementation

*(See Report of the 4-5 December 2014 Advisory Board Meeting, paras 21 and 116-117))*

3. Philippe Lortie indicated that, although it had been noted that the implementation of the application in the Cloud would be significantly less expensive, there was a strong preference amongst the Advisory Board members for a local implementation. The Cloud is not yet considered mature enough to possibly allow sensitive data to rest in an application, even for a very short time, in the Cloud. It was also clear that an iSupport database could not rest in the Cloud in the light of the very sensitive data contained therein.

4. The Working Group supported that conclusion.

**Secure communications (e-codex)**
*(See Report of the 4-5 December 2014 Advisory Board Meeting, paras 97-105 and 122-124)*

5. Philippe Lortie gave a short overview of the Secure Communication (e-CODEX) Working Group conclusions, and indicated that e-CODEX[1] was recommended as the most secure means to electronically communicate and exchange data within Europe. He added that e-CODEX is now being used by non-EU-member States, such as Australia, New Zealand, Norway or Turkey. The Secure Communication (e-CODEX) participants from States outside Europe, such as Brazil and the United States of America are currently assessing the possibility of using e-CODEX in the context of iSupport and will give their final assessment on the use of e-CODEX before the end of February.

**Access rights and user profiles**
*(See Report of the 4-5 December 2014 Advisory Board Meeting, paras 83-86 and 119-121)*

6. Philippe Lortie drew the attention of the experts to the strong legal and practical framework established by both the 2009 Regulation and the 2007 Convention in relation to data protection. Mandatory forms and recommended forms have been adopted under the 2009 Regulation and the 2007 Convention. Specific provisions with regard to data protection conditions are set-out in the 2009 Regulation. Philippe Lortie pointed out that the type of data that might be exchanged between Central Authorities, the conditions of use and the duration of data storage by national authorities are set out in Article 61 and Article 62 of the Regulation. He observed that a greater protection is provided under the 2007 Convention in the event of domestic violence issues.

7. Philippe Lortie stated that access to the iSupport system will be provided on the basis of a user name and password. States having additional login requirements (biometrics, token) were invited to describe such requirements. Implementation of additional requirements will be the responsibility of each State.

8. With regard to "user profiles", the iSupport Functional Requirements Working Group will discuss and set up different types of profiles on the basis of the extent and the type of information different actors can have access to (for example: "manager", "case-worker", "enforcement officer").

**External access**
*(See Report of the 4-5 December 2014 Advisory Board Meeting, paras 87-89)*

9. With regard to external access, Philippe Lortie mentioned that third parties such as Judges, enforcement officers or government agents could have access to iSupport. External access shall also be secured and based on credentials, using a SSL connection in the event of a web base application or a VPN if connecting directly to the main frame. Further discussions on the actors involved and the type of data accessible will take place within the iSupport Functional Requirements Working Group.

10. In response to a question from an expert from Estonia, Philippe Lortie pointed out that the responsibility to give access rights and to allocate profiles will be the responsibility of the Central Authority. Within the Central Authority, an administrator will have access to the back end of iSupport and set up these access rights, credentials and profiles.

[1] E-CODEX documentation is available on the website of the Hague Conference at < www.hcch.net > under the "iSupport Specialised Section" then "Secure Communications (e-CODEX) Working Group (3)" and "Documents for 12 January 2015 Meeting".

11. In response to a question from an expert from Brazil, Philippe Lortie explained that the messages exchanged between Central Authorities will not be associated with a specific case worker, but with a case number. Furthermore, as soon as a Case Worker has ceased employment with the Central Authority, this caseworker will be unable to receive any messages from another Central Authority as his / her user account will be disabled.

**Integration with existing national systems / interface / web-services**
*(See Report of the 4-5 December 2014 Advisory Board Meeting, paras 112-114)*

12. Philippe Lortie noted that the proportion of international cases is rather small in comparison to national cases. He stressed that most States will most likely not integrate iSupport with their national system but rather use it in parallel with a plugin allowing the import and export of data from the national database to the iSupport system. He pointed out, however, that iSupport would not have access to the national system and that the transferred data would exclusively consist of specific pre-identified data. Furthermore, the responsibility of connecting a national system to iSupport would be the responsibility of each State.

**Logging of changes and views / "time-stamp" / "audit trail"**
*(See Report of the 4-5 December 2014 Advisory Board Meeting, par. 115)*

13. Philippe Lortie stressed the relevance of this topic for the participating States. He pointed out that each Central Authority will want to be able to verify *post facto* the persons who have viewed or edited any data, and when that was done. He noted however that there is no consensus on the level of detail required for collecting and storing such data. He stressed the importance of first setting out, on a rather detailed basis, a common framework for this collection and storage. He then mentioned the possibility that in a second phase, depending on resources available, a flexible system could be provided that would allow lower levels of detail to be set up for interested States.

**Web-browsers and web-based systems**
*(See Report of the 4-5 December 2014 Advisory Board Meeting, paras 90-93)*

14. Philippe Lortie first recalled that the iSupport system will be implemented within the local IT infrastructure of each State and that access to the local servers would be provided using commonly available web-browsers. Philippe Lortie pointed out that the web browsers used to access the iSupport system should be regularly updated to respond to security risks.

15. It was noted however that many different web-browsers are being used around the world. Philippe Lortie recommended that following the iSupport Advisory Board advice, the iSupport system should operate if possible on the latest two versions of the three most commonly used web-browsers. However, depending on the resources available, access could possibly be limited to only two different web-browsers. A first Questionnaire has provided valuable guidance on this matter but was limited to 26 Countries. A continued collection of information about web-browsers used by other States will probably be necessary.

**Access to external websites**
*(See Report of the 4-5 December 2014 Advisory Board Meeting, paras 94-95)*

16. Philippe Lortie presented one key result of the Survey relating to this topic. In some governments access to the web is restricted or even prohibited, mostly to avoid external intrusion. He stressed that some very useful information was available on the Internet, and that amongst other possibilities, iSupport could provide for these documents in a PDF format, or give access to specific designated

websites. . Philippe Lortie recommended further investigation to determine the most convenient and cheapest solution.

17. An expert from the United States of America underlined that it was important that these links not come back into the application (i.e., iSupport) but in a separate browser.

**Database encryption**
*(See Report of the 4-5 December 2014 Advisory Board Meeting, par. 96)*

18. Philippe Lortie suggested circulating amongst iSupport national points of contact a questionnaire to collect information on the encryption of their national database, and on any legal obligations related to encryption. On the basis of the result of this Questionnaire, the Working Group will decide whether encryption of the database should be an option.

**European Data Protection Regulation**

19. Philippe Lortie observed that a proposal for a European Data Protection Regulation is currently being discussed by the Council and the Parliament of the European Union. He added that 2009 Regulation also provides the obligation to inform the data subject about any collected data within 90 days. Philippe Lortie accordingly suggested adding to iSupport a functionality reminding the caseworker about this notification requirement. The discussion in the group revealed that other States outside Europe have similar notification requirements.

20. Philippe Lortie also addressed the right of the Data Subject to obtain the erasure of collected personal data when it is no longer required in relation to the purposes for which it was collected. Philippe Lortie specified that the ability to delete data under very specific conditions will be limited to the administrator under the leadership of the manager.

**Data protection officer / access to information officer**
*(See Report of the 4-5 December 2014 Advisory Board Meeting, par. 85)*

21. Philippe Lortie stressed the importance of involving access to information officers or data protection officers in the iSupport project. He invited experts to make contact with these persons in their department or Ministry and to obtain and report to the Working Group any relevant information or advice those officers may have with regard to other data protection issues.

**Privacy impact assessment / security scans during the development process (data protection certificate)**
*(See Report of the 4-5 December 2014 Advisory Board Meeting, paras 85 and 96)*

22. Philippe Lortie suggested that security scans of the system should be undertaken by experts during the development phase (*i.e.*, programming stage). He stressed the importance of addressing any data protection issue in a timely fashion, in order to meet the requirements of any privacy impact assessment that needs to be conducted in a State before the system is implemented. Accordingly, he invited all experts present to designate experts in this area with a view to finding volunteers that could assist with the security scans during the development stage.

23. Experts supported the findings of the iSupport Team as the way forward with regard to data protection.

**III. QUESTIONS AND CLOSING REMARKS**

24. An expert from Estonia raised the issue of the duration of audit trail retentions, and asked if the audit trail would be stored for the same duration as the data itself.

25. Philippe Lortie answered that the duration of data retention will be governed by the national law. He added that the functionality Working Group will have the opportunity to discuss the different statuses of a case (such as archived, open, closed). With regards to the audit trail, the duration of retention will certainly be technically limited by the size of the database. If it were necessary to keep the log forever, it will be important to make certain that the State's iSupport database can manage the increasing volumes of data or to have the archived data stored in another database.

26. An expert from the United States of America indicated that their audit trails were kept for 3 to 5 years, depending on the type of data.

27. An expert from the National Child Support Enforcement Association indicated that in her State the logs could not be separated out from the rest of the information. She expressed the need to differentiate between the legal requirements of retention with regard to, respectively, the audit logs and the personal data. That distinction will be useful with regard to the design of the system.

28. An expert from Estonia stated that in his State audit trails relating to data change were kept for the same duration as the data itself, while access logs were retained for a shorter period.

29. In response to another question from expert from Estonia, Philippe Lortie specified that the audit trails would be retained in the local database as well.

30. In closing, Philippe Lortie welcomed any further contribution before the next meeting with regard to non-addressed issues.