Serectrix s.n.c.
di Di Iorio & C.
Via S.Lucia 3/D, 65010 Spoltore (PE) – ITALY
Tel./Fax: +39 085 4429188

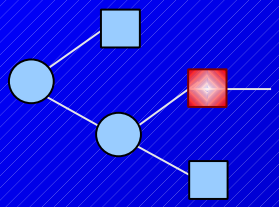
B.I.R.O.

WP 5

"THE PRIVACY IMPACT ASSESSMENT PROCESS"

Dr. Concetta Tania Di Iorio

tania_diiorio@virgilio.it



THE PIA PROCESS

The PIA process includes **4 steps**:

- **Step 1: Preliminary PIA**
- **Step 2: Data flows Analysis**
- **Step 3: Privacy analysis**
- **Step 4: PIA Report**

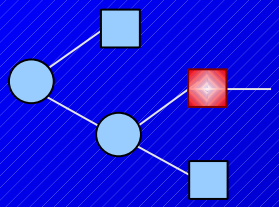
STEP 1: PRELIMINARY PIA

Objectives:

- To highlight significant privacy risks in the management of the BIRO Information System
- To identify the main alternatives for the development of BIRO through a review of the literature

Step 1 Final Report will include:

- Introduction/Project Background and Description
- Legislative and Policy framework
- Description of Personal Information (required level of data aggregation and data flow)
- Potential Privacy Risks
- Overview of Security Requirements

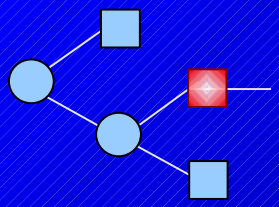


STEP 1: PRELIMINARY PIA

PRIVACY FACILITATOR

<u>The Privacy Facilitator</u>:

- **will be responsible for the completion** of both the **Preliminary** and the **Full PIA**
- **will assist the consortium throughout the entire process on legal and privacy issues**

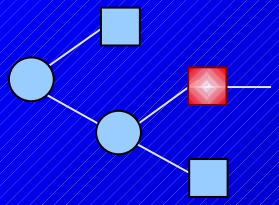


STEP 1: PRELIMINARY PIA
THE PIA TEAM

<u>The PIA Team includes</u>:

- **The privacy facilitator**
- **Other PIA Team Members, to be designated,** with the following expertise:
  - **Technology and systems expertise**
  - **Information and records keeping skills**

All partners should be represented in the PIA Team

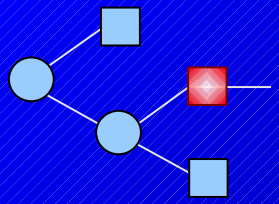


STEP 1: PRELIMINARY PIA

PIA TEAM TASKS (1)

The privacy facilitator will provide **:**

- An indication of **selected papers**, extracted **from the relevant scientific literature** by May 2006
- A technical report (**Draft Preliminary PIA**) by June 2006
- The **final version of the Preliminary PIA** by 1st December 2006

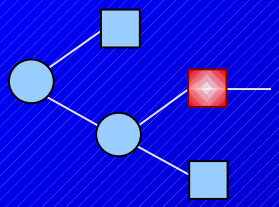


STEP 1: PRELIMINARY PIA

PIA TEAM TASKS (2)

The PIA Team members should:

- **Review the literature selected by the privacy facilitator/PIA Team members**
- Identify a **checklist** of relevant features that will be classified into key **privacy requirements** for **the BIRO information system**
- Select a **limited number (N=3) of candidate alternative architectures** for the



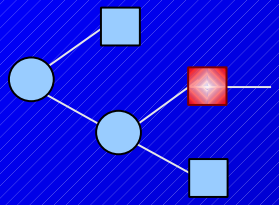
STEP 1: PRELIMINARY PIA
LEGISLATIVE FRAMEWORK

- **EU legislation**:
  - Directive 95/46/EC
  - Directive 2002/58/EC
  - Treaty of the European Union (Art. F)Article F
  - EU Convention Protection of Human Rights (Art. 8)
  - EU Charter of Fundamental Rights (2000)
- **Council of Europe:**
  - Convention 108/88;
  - Recomm. R(99)5 & R(97)5
  - Convention on Biomedicine(1997))5
- **OECD:**
  - Guidelines on Security of Information Systems;
  - Guidelines on Privacy
- **United Nations**:
  - Universal Declaration of Human Rights (Art XII);
  - UN Guidelines on computerized personal data file;
  - Int. Covenant on Civil and Political Rights (Art. 17)

STEP 2: DATA FLOW ANALYSIS

Overview:

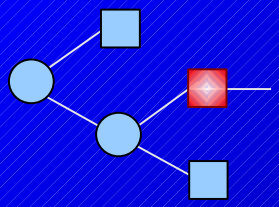
- The activity consists of a description and in depth **analysis of the selected alternatives for the BIRO system**
- The purpose of this step is to **rank the alternatives** through the detailed description of the personal information flow
- Instruments:
  - **Information Flow Diagram**
  - **Data Flow Table**



STEP 2: DATA FLOW ANALYSIS

THE INFORMATION FLOW DIAGRAM

- Identifies how information flows within and across registers, and between the different centres and the central engine
- Provides the **"big picture" of the BIRO system**
- The diagram should identify, at a general level:
  - the major components of the processes
  - how personal information is collected, used, disclosed and retained throughout the process



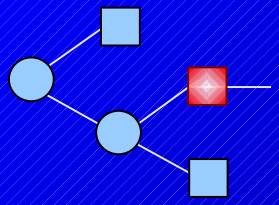
STEP 2: DATA FLOW ANALYSIS

DATA FLOW TABLE

The Data Flow Table **follows each data element** or cluster **from the collection, use, and disclosure, to the final disposition**

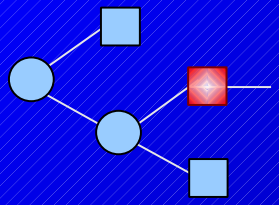
Data Flow Table

Description of personal information cluster	Collected by	Type of format (e.g. paper, electronic	Used by	Purpose of collection	Disclosed to	Storage or retention site



STEP 2: DATA FLOW ANALYSIS
PANEL RANKING FORM

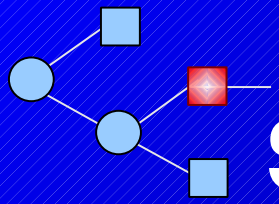
- List of all key questions from step 1 (yes/no)
- Each question contributing to one dimension (criterion)
- Mark for each dimension equal to the standardized sum of yes/no for all questions
- Summary marks for each dimension/alternative/panelist reported on a panel summary report



STEP 2: DATA FLOW ANALYSIS

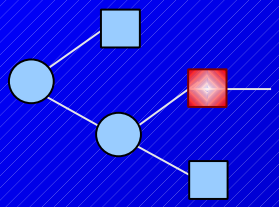
TASKS

- **The PIA Team** will evaluate each alternative against agreed privacy criteria (step 1), including PETs
- **The facilitator** will set up a **consensus panel** (modified Delphi Panel):
  - a mark will be assigned for each criterion for all alternatives
  - **alternatives will be ranked**
  - **best privacy enhancing system architecture will be identified by April 2007**
- **The facilitator** will provide the **Data Flow Report**



STEP 3: PRIVACY ANALYSIS

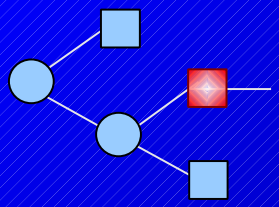
- The privacy analysis **examines the data flows of the selected BIRO architecture in the context of applicable privacy policies and legislation**
- **A detailed questionnaire is used to facilitate the identification of major privacy risks**
- The privacy analysis derives from **yes/no responses to a series of questions**



STEP 3: PRIVACY ANALYSIS QUESTIONNAIRE (EXAMPLE 1)

1. Accountability for Sensitive Information

Questions For Analysis	Yes	No	N/D N/A	Provide Details
1.1 Has responsibility for privacy been assigned?				
1.2 Has the custody and control of sensitive information been determined?				
1.3 Has the accountability of the program custodian of sensitive information been documented?				
1.4 Are third parties involved in the custody or control of sensitive information?				
1.5 If third parties are involved, do you have an agreement in place that establishes privacy requirements?				

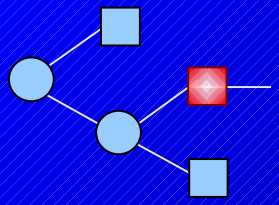


STEP 3: PRIVACY ANALYSIS

QUESTIONNAIRE (EXAMPLE 2)

2. Collection of Sensitive Information

Questions For Analysis	Yes	No	N/D N/A	Provide Details
2.1 What is your authority to collect sensitive information?				
2.2 Is sensitive information collected directly related to the project?				
2.3 Is sensitive information being collected directly from the individual?				
2.4 Is all sensitive information collected necessary to the project?				
2.5 Are secondary uses contemplated for the information collected?				
2.6 Is information anonymized when used for planning, and/or evaluation purposes?				
2.7 Does the project involve the collection through a common patient identifier?				



STEP 3: PRIVACY ANALYSIS

TASKS

- The privacy facilitator:
  - will distribute a **questionnaire** to the PIA Team by Sep. 2007
  - will highlight the major **vulnerabilities** and **privacy risks**
  - will solicit the PIA team to develop **possible solutions for each privacy risk** (**summary tables** could be used)
- The PIA Team will **revise the BIRO system** accordingly (draft Report by Dec 2007)
- The **privacy facilitator** will produce the **Privacy**

STEP 3: PRIVACY ANALYSIS

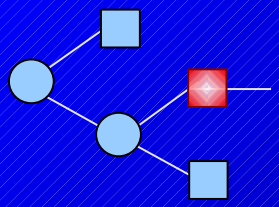
EXAMPLE OF SUMMARY TABLE

Summary Table						
Element	Nature of risks	Level of risks			Comments	Mitigating Mechanisms
		Low	Medium	High		

STEP 4: PIA REPORT

The PIA Report:

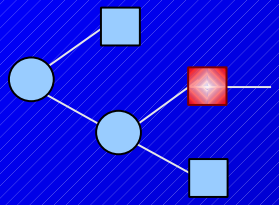
- **is a documented evaluation of the privacy risks and associated implications**, along with a discussion of possible **remedies or mitigation strategies**
- includes an **accompanying action plan** to ensure that privacy is managed effectively during the maintenance of the BIRO Information System
- **will be provided by the privacy facilitator by**



STEP 4: PIA REPORT

TABLE OF CONTENT

- **Executive Summary**
- **Introduction**: Report Objectives, Scope of PIA, Reference Documentation, Participants
- **Project Description**
- **Data Flow Analysis**: Information Flow Diagram and Description, Data Flow Table
- **Privacy Analysis**
- **Privacy Risk Management Plan**: Privacy Risk Mitigation, privacy risk (1-n), Summary Table
- **Communication Strategy**



WP 5 DELIVERABLES

- Preliminary Privacy Impact Assessment Report *(November 2006)*
- Data Flow Analysis Report *(June 2007)*
- Privacy Analysis Report *(February 2008)*
- Privacy Impact Assessment Report *(July 2008)*