Standard Project Fiche 2005  
for Phare assistance

1. Basic Information

1.1 CRIS Number: BG 2005/017-586.03.01

1.2 Title: Further Strengthening of the Administrative Capacity of the Bulgarian Commission for Personal Data Protection and providing conditions for implementation of the Personal Data Protection law.

1.3 Sector: Justice and Home Affairs

1.4 Location: Republic of Bulgaria, Commission for Personal Data Protection

1.5 Duration: Twinning – 12 months

2. Objectives

2.1 Overall Objective(s):

Strengthening the Commission for Personal Data Protection (CPDP) in accordance with the EU best practices through institution building and investments.

2.2 Project purpose:

To achieve higher effectiveness of personal data protection activities by adoption and implementation of the best practices in prevention and protection.

2.3 Accession Partnership (AP), Catalogue of main administrative structures for the implementation of the acquis, Roadmap for Bulgaria, NPAA.

2.4 Coherence with National Development Plan (and/or Structural Funds Development Plan) - N/A

2.5 Cross Border Impact - N/A

3. Description

3.1 Background and justification:

Personal data protection law has been enforced since 1 January, 2002. /promulgated in the State Gazette, issue 1 dated 4 January, 2002./.

The Commission for Personal Data Protection /CPDP/ is an independent state authority which ensures protection of people in processing their personal data and in giving the access to these data, as well as the control on observing the Personal Data Protection Law /PDPL/. It is a juridical entity funded by the budget with a head office in Sofia city.

The Chairman and the Commission’s members were elected by the Parliament at the proposal of the Council of Ministers on 2002.
In compliance with Art. 2, par. 3 of the Transitional and Final Provisions of the PDPL within three months since the election of the Commission it shall adopt and promulgate in the State Gazette the Rules on its activities and administration. Art. 2, par. 4 of the Transitional and Final Provisions of the PDPL regulates the liability of the Council of Ministers to provide the necessary property and financial resources for the start of the Commission’s work within one month after the decision of the Parliament for election of the Commission members.

These two provisions of the PDPL, though they are enforced for a limited time, are of great importance for the institutional building of the CPDP because they are directly connected with the formation of two main components as a juridical entity – its property and staff.

Unfortunately the obligation of the Council of Ministers for equipment of CPDP with appropriate building was not fulfilled neither in the one month period stipulated in Art. 2, par. 4 of the Transitional and Final Provisions of PDPL nor until the present moment. This problem was also set out in the Regular Reports for 2003 and 2004 of the EC as one of the main recommendations for the Commission’s work. The temporary decision which the Commission made, in the beginning of 2005, was to lease a building – private property. If this problem persists the normal work of the Commission and its administration will be endangered.

The first Rules on CPDP’s activities and its administration were issued and promulgated in the State Gazette on 23.07.2002. On 31.01.2003 the new Rules on CPDP’s activities and its administration were issued and promulgated in the State Gazette, these Rules are still in power.

With a view to the institutional development and improvement of the work of the Commission it is necessary:

- The implementation of an effective system of control over the controllers of personal data;
- To build a national network of CPDP on the territory of the Republic of Bulgaria;
- To qualify and train the staff of CPDP competent with legal, technical and organizational questions, concerning practical implementation of personal data protection in the EU member states, in place from 2006 to 2007;
- To further develop the HQ and to build 6/six/ Regional offices of CPDP

At present in CPDP and its administration 31 officers are employed and the total number of the employees according to the Rules of the CPDP is 76, the number of the staff is to be increased to 129 officers.

In order to execute its powers under PDPL, the Commission holds regular or additional sessions, carries out inspections on complaints made or in case of self-appointment it expresses opinions, organizes seminars, working meetings and discussions.

CPDP is conducting database of the controllers of personal data and the databases they control. In connection with this, CPDP on one of its sessions had published in the Country paper a model of application for registration of a controller of personal data as well as an annex with a description for the database they control.

The lack of appropriate building for the activities of CPDP from its creation to the present moment made it impossible to develop its full administrative capacity, to
develop its informational infrastructure and to create needed specialized software, forced the Commission to apply for this PHARE project.

The proposed project is corresponding with the recommendations in the EC Report for Bulgaria in 2004, as well as the last warning letter from 09.06.2005 of the EC for the fields in which Bulgaria must take emergency measures before its accession to the EU in 2007.

Thus CPDP will have the opportunity to meet all main requirements of the Directive 95/46/EC and Convention 108 of the Council of Europe.

3.2 Sector rationale
N/A

3.3 Results

Component 1 – Institution Building
Result No 1
• Implementation of an effective system of control over the controllers of personal data.
   Result No 2
• Building an information system of CPDP on the territory of the Republic of Bulgaria;
   Result No 3
• Qualified and well-trained CPDP staff with full knowledge of legal, technical and organizational questions concerning practical implementation of personal data protection in the EU member states; in place from 2006 to 2007
   Result No 4
• Building-up the HQ and 6/six/ Regional offices of CPDP;
   Result No 5
• Building a local network infrastructure of CPDP on the territory of the Republic of Bulgaria

Component 2 – Investment Support
Result No 6
• Technical, information and other equipment for effective protection of the network infrastructure and information system of CPDP from unauthorized access;
   Result No 7
• Supply of the equipment necessary for the completion and launch of the CPDP training center.

3.4 Activities

The above results will be achieved by implementing the following activities:

Component 1 – Institution Building
Activity No 1
• Development of a Guideline of procedures for control over the controllers of personal data
   Activity No 2
• Training of the CPDP administration in legal, technical and organizational questions concerning practical implementation of the Personal Data Protection Law
   Activity No 3
• Assessment of the training needs of the staff of CPDP;
Activity No 4
• Development of Guideline for training personal data controllers on the implementation of Personal Data Protection Law

Activity No 5
• Basic training of the new recruited staff of the 6/six/ regional offices concerning practical implementation of the Personal Data Protection Law.

Activity No 6
• assistance for assessing the needs in view of the development of the network infrastructure – to be performed during the twinning project.

Activity No 7
• Consulting assistance for development of a working and technical project for information system of the register of controllers of personal data by making a website and information bulletin of CPDP – to be performed during the twinning project.

Activity No 8
• System of communication with the users by developing a website and information bulletin of CPDP.

Activity No 9
• Preparation of an assessment for the needs of CPDP in terms of IT, communication and security of data

Component 2 – Investment Support

Activity No 10
• Supply of specialized equipment and software for the needs of CPDP;

Activity No 11
• Supply of the necessary technical and office equipment for the 6/six/ regional offices;

Activity No 12
• Supply of the technical and office equipment for the Training Center of CPDP.

3.5 Linked Activities:
This is the first project of the Commission on personal Data Protection financed under Phare or other donors.

3.6 Lessons learned:
The aim of this project is to address the needs identified in the Regular Report 2004 for strengthening of the administrative capacity of the Commission for Personal Data Protection. In order to implement the project successfully the CPDP will learn from the extensive experience of other Bulgarian Institutions – e.g. Ministry of Interior, with projects funded under Phare. The necessary co-operation with such institutions was ensured at the initial stage of designing of the project fiche.

4. Institutional Framework

The Commission for Personal Data Protection will be the beneficiary of the project. The overall project coordination and implementation will be entrusted to Member of the Commission and a steering committee. In order to develop effective coordination in the project implementation, CPDP will ensure adequate leadership team in charge of all issues related with the project’s implementation and coordination.
The Chairman of the Steering committee will be:
Mr. Ivo Stefanov, President of CPDP
1 Dondukov Blvd., Sofia
tel. (+359 2) 940 20 46
Commission for Personal Data Protection will closely cooperate with CFCU within the Ministry of Finance and DEC.
A Steering Committee will be set up in order to guarantee the effective co-ordination of the project.

The Committee will be responsible for:
- approving the decisions taken in the course of project activities;
- providing guidelines to the working groups set up under this project;
- providing all the information necessary for project implementation;
- taking prompt measures in view of ensuring smooth implementation of the project in cases of delay or other unforeseen obstacles;

The Steering Committee will meet every six months and if necessary, on an ad hoc basis.

5. Detailed Budget

<table>
<thead>
<tr>
<th>€M</th>
<th>Phare/Pre-Accession Instrument support</th>
<th>Co-financing</th>
<th>Total Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>National Public Funds (*)</td>
<td>Other Sources (**)</td>
<td></td>
</tr>
<tr>
<td>Year 2005 - Investment support jointly co funded</td>
<td>0.500</td>
<td>0.167</td>
<td>0.167</td>
</tr>
<tr>
<td>Contract 2</td>
<td>0.500</td>
<td>0.167</td>
<td>0.167</td>
</tr>
<tr>
<td>Investment support – sub-total</td>
<td>0.500</td>
<td>0.167</td>
<td>0.167</td>
</tr>
<tr>
<td>% of total public funds</td>
<td>75 %</td>
<td>25 %</td>
<td></td>
</tr>
</tbody>
</table>

| Year 2005 Institution Building support | | | |
| Contract 1 – Twinning | 0.700 | | 0.700 |
| IB support | 0.700 | | 0.700 |
| Total project 2005 | 1.200 | 0.167 | 1.367 |

(*) contributions form National, Regional, Local, Municipal authorities, FIs loans to public entities, funds from public enterprises
(**) private funds, FIs loans to private entities
National co-financing of up to 10 % of the PHARE twinning support will be ensured by National Fund Directorate, Ministry of Finance. National co-financing will be ensured in the form of joint co-financing with PHARE funds.
6. Implementation Arrangements

6.1 Implementing Agency

The CFCU within the Ministry of Finance is the Implementing Agency. The CFCU will be responsible for tendering, procurement of equipment and financial control during the implementation of the project. CPDP will co-ordinate the elaboration of technical specifications, nominate experts to participate in the evaluation of offers and monitor the delivery, installation and configuration of equipment.

6.2 Twinning

The project implementation will start with the twinning contract including a RTA and one Project Leader level expert (to conceive, supervise and coordinate the project). For the implementation of this project Resident Twinning Advisor and short-term experts from the EU member states will be needed. The Resident Twinning Advisors should be a middle or senior ranking official with profound knowledge and experience in the field of the personal data protection. The Resident Twinning Advisor will be expected to establish and maintain good relations with the CPDP officials in order to fully understand their views and be in position to transfer effectively ideas and techniques. This implies that the Resident Twinning Advisor should be professionals with good communication skills.

The Twinning Resident Advisor is expected to have good knowledge in the following areas:

- Legal aspects (general functioning of personal data protection, EU legal instruments – Directive 95/46/EC, and other relevant JHA acquis);
- Experience with Information systems for data protection will be considered as advantage.

The Resident Twinning Advisor should be able to provide effective support in developing training programs. He will also provide advice for the development of a countrywide IT network based on the functioning needs of CPDP offices. Very good knowledge of English, both oral and written, is required.

Project Leader (SPO for the entire Project including the twinning sub-project):

**Mr. Krasimir Dimitrov**
Member of the CPDP
1 Dondukov Blvd., Sofia
Tel.: (+359 2) 9402046

Project Coordinator:
Mr. Stoyan Tsanov
Director of P T Directorate
1 Dondukov Blvd., Sofia
Tel.: (+359 2) 9153508

6.3 Non-standard aspects

None. The project will be implemented in compliance with the Practical Guide to contract procedures financed from the general budget of the European Communities in the context of external actions (PRAG) and in accordance with the guidelines contained in the Twinning Manual (May 2005) and the Phare Programming Guide 2005.
Bulgarian co-financing will be provided for by the national budget through the National Fund Directorate within the Ministry of Finance. Bulgarian co-financing will be contracted along with the amounts allocated under Phare Program.

6.4 Contracts
The contracts envisaged under the project will be contracted and implemented according to the PHARE rules. The estimated number of contracts is as follows:

**Contract 1- Twinning** - 700 000 €
**Contract 2 - Supply** of technical and office equipment for the needs of CPDP - 667 000 €

7. Implementation Schedule

7.1 Start of tendering/call for proposals

(call for proposals regarding
/i/ the selection of twinning partner, and
/ii/ preparation of procurement)

- approval of programme – December 2005;
- selection of twinning partner – December 2005;
- start of twinning activities – July 2006

7.2 Start of project activity – 2005

7.3 Project completion – December 2007

8. Equal Opportunity

During the implementation of the project the CPDP will guarantee equal opportunities for participation of men and women.

9. Environment

The project investments comply with EU norms and standards. They will not have adverse effects on the environment.

10. Rates of return

A rate of return analysis is not applicable to the project. After realization the project will have operational effect in the field personal data protection.

11. Investment criteria (applicable to all investments)

11.1 Catalytic effect

Adoption and application of the European acquis in the field of justice and home affairs is an essential element of the general process of Bulgaria’s preparation for accession to EU. Phare investment will support the improvement of personal data protection legislation, the enhancement of capacity to use and exploit centralized information systems and the improvement of the effectiveness of the work of CPDP.
11.2 Co-financing

Bulgarian authorities will provide 25% as co-financing for the project investment component.

11.3 Additionality

This project has no financial return to attract private or international sources of funds.

11.4 Project readiness and size

11.5 Sustainability

Project’s purpose – results expected – activities to deliver results are conceived and designed to bring sustainable modernisation and optimisation of the function and management of personal data protection together with lasting compliance with relevant EU acquis and best practice in MS.

11.6 Compliance with state aids provisions – N/A

12. Conditionality and sequencing

Bulgarian authorities will continue to demonstrate commitments to adopt and implement the EU acquis in personal data protection leading to a modern, transparent, human rights minded and citizens-oriented culture in CPDP. Before the practical start of implementation of the project the tasks and responsibilities of all involved services will be defined and approved. In this connection, considerable experience has already been gained in making such arrangements. At this stage the services involved have already exchanged preliminary information about future project implementation and the respective division of tasks/responsibilities.

Since the Project will be implemented through a twinning this will require full commitment and involvement on behalf of senior level officials of the beneficiary institution. Therefore, the leadership of the CPDP commits to provide adequate staff and support to the twinning partner (incl. translation and interpretation) as well as to introduce the institutional changes identified as needed for the successful implementation of the project. CPDP will ensure that all conditions necessary for DEC control over Project implementation as well as Project steering are in place. Throughout the Project implementation all MS and PDP experts will have the adequate access to all managerial levels required.

In cases of unforeseen delay of project implementation or other obstacles, the leadership of the CPDP together with the twinning partner will define and undertake the necessary measures for overcoming them.

ANNEXES TO PROJECT FICHE

1. ANNEX 1 Logframe in standard format
2. ANNEX 2 Detailed implementation chart
3. ANNEX 3 Contracting and disbursement schedule, by quarter, for full duration of project
4. ANNEX 4 Needs Assessment
5. ANNEX 5 Building a local national Network of CPDP on the territory of the Republic of Bulgaria.
6. ANNEX 6 Reference list of relevant laws and regulations.
7. ANNEX 7 Indicative list of equipment
## LOGFRAME PLANNING MATRIX FOR

**Further Strengthening of the Administrative Capacity of the Bulgarian Commission for Personal Data Protection and providing conditions for implementation of the Personal Data Protection law.**

<table>
<thead>
<tr>
<th>Program name and number</th>
<th>Contracting period expires: 30 November 2007</th>
<th>End of execution of contracts expires: 30 November 2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>BG</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Overall objectives</th>
<th>Objectively Verifiable Indicators</th>
<th>Sources of Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Strengthening the Commission for Personal Data Protection (CPDP) In accordance with the EU best practices through Institution building and investments.</td>
<td>- CPDP fully operational and completely complying with relevant EU aquis; - Recruitment of the necessary staff; - Transparent rules for collection and processing of personal data; - Personal Data Protection (PDP) regulatory mechanisms developed and in place by the end of 2007; - Increasing the number of officers trained for realization of control activity of CPDP and preparation of compulsory recommendations for</td>
<td>- European Commission Regular Report; - Internal legislation in field of Personal data Protection; - Other official documents, analyses and reports worked out by the European Commission and the Bulgarian authorities.</td>
</tr>
</tbody>
</table>

| Total budget : 1 367 000 EUR | Phare budget : 1 200 000 EUR |
administrators in connection with personal data protection.

<table>
<thead>
<tr>
<th>Project purpose</th>
<th>Objectively Verifiable Indicators</th>
<th>Sources of Verification</th>
<th>Assumptions</th>
</tr>
</thead>
</table>
| - Institutional building /IB/ and IB-related investments in the CPDP of Bulgaria - to achieve a higher effectiveness & better efficiency of the personal data protection /PDP/ activities in the country by the adoption and implementation of EU best practices in prevention of PDP violations and for best protection of personal data. | - EU compliant rules and procedures for collection and processing of personal data in place by 2007;  
- Enhancement of the staff of the CPDP in connection with the implementation of Personal Data Protection law;  
- Training courses for the staff of CPDP in connection with the new IT equipment;  
- CPDP fully operational and completely complying with relevant EU acquis. | - Reports of the RTA;  
- Report of the Project Steering Committee;  
- Reports of MS STE missions;  
- CPDP Reports. | - Full implementation of the Personal Data Protection (PDP) legislation in the Republic of Bulgaria in accordance with the EU requirements and standards. |

<table>
<thead>
<tr>
<th>Results</th>
<th>Objectively Verifiable Indicators</th>
<th>Sources of Verification</th>
<th>Assumptions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Institutional building</strong></td>
<td><strong>Investment support</strong></td>
<td><strong>Other support measures</strong></td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------</td>
<td>---------------------------</td>
<td></td>
</tr>
<tr>
<td>- System of effective nation-wide control over the controllers of personal data implemented / introduced / by 2006/2007;</td>
<td>- Technical, information and other equipment for effective protection of the network infrastructure and information system of CPDP from unauthorized access;</td>
<td>- Amendments to the Personal Data Protection Law and the related bylaws;</td>
<td></td>
</tr>
<tr>
<td>- Building a local network infrastructure of CPDP on the territory of the Republic of Bulgaria;</td>
<td>- Supply of the equipment necessary for the</td>
<td>- Adequate support of the activities by the national budget;</td>
<td></td>
</tr>
<tr>
<td>- Building an information system of CPDP on the territory of the Republic of Bulgaria;</td>
<td>- Full technical equipment and modernization of the administration of CPDP;</td>
<td>- Controllers of personal data interested in participation in the training courses.</td>
<td></td>
</tr>
<tr>
<td>- Qualified and well-trained CPDP staff with full knowledge of legal, technical and organizational questions concerning practical implementation of personal data protection in the EU member states; in place from 2006 to 2007;</td>
<td>- Purchase of a high precision system with specialized software for management of the access of the end users to the information infrastructure of CPDP;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Building-up the HQ and 6 /six/ Regional offices of CPDP.</td>
<td>- Building of a training centre for the staff of CPDP and the controllers of personal data;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Up to 1% of the controllers of personal data trained;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- All of the existing staff of CPDP trained;</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Workshops, seminars and training in new devices, technical and normative acts.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Activities</td>
<td>Means</td>
<td>Assumptions</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-------</td>
<td>-------------</td>
<td></td>
</tr>
</tbody>
</table>
| **Institution Building** | - A Twinning project with an EU member state;  
- Implementation of the Twinning contract;  
- Contracts for supply of the equipment needed; | - Involvement of the CFCU at the Ministry of the finance during tendering and contracting procedures;  
- Adequate training of the executive personnel in the system’s operation. |
| - Assessment of the training needs of the staff of CPDP;  
- Basic training of the new recruited staff of the 6/six/ regional offices concerning practical implementation of the Personal Data Protection Law and the best EU aquis practices;  
- Training of the CPDP administration in legal, technical and organizational questions concerning practical implementation of the Personal Data Protection Law and the best EU aquis practices;  
- Development of a Guideline of procedures for control over the controllers of personal data.  
- Development of Guideline for training personal data controllers on the implementation of Personal Data Protection Law. |
- Consulting assistance for development of a working and technical project for the network infrastructure;

- Consulting assistance for development of a working and technical project for information system of the register of controllers of personal data by making a website and information bulletin of CPDP;

- System of communication with the users by developing a website and information bulletin of CPDP;
- Preparation of an assessment for the needs of CPDP in terms of IT, communication and security of data.

**Investment support**
- Supply of specialized equipment and software for the needs of CPDP;

- Supply of the necessary technical and office equipment for the 6 /six/ regional offices;

- Supply of the technical and office equipment for the Training Center of CPDP.
## ANNEX 2

### DETAILED IMPLEMENTATION CHART

<table>
<thead>
<tr>
<th></th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1&lt;sup&gt;st&lt;/sup&gt; Q</td>
<td>2&lt;sup&gt;nd&lt;/sup&gt; Q</td>
<td>3&lt;sup&gt;rd&lt;/sup&gt; Q</td>
<td>4&lt;sup&gt;th&lt;/sup&gt; Q</td>
</tr>
<tr>
<td><strong>Institution building</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contract 1 – Twinning</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Investment</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contract 2 – Supply</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

T – Tendering;  
C – Contracting;  
I – Implementation;
### ANNEX 3

**CONTRACTING AND DISBURSEMENT SCHEDULE, BY QUARTER, FOR FULL DURATION OF THE PROJECT**

<table>
<thead>
<tr>
<th>Year</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarters</td>
<td>1&lt;sup&gt;st&lt;/sup&gt; Q</td>
<td>2&lt;sup&gt;nd&lt;/sup&gt; Q</td>
<td>3&lt;sup&gt;rd&lt;/sup&gt; Q</td>
<td>4&lt;sup&gt;th&lt;/sup&gt; Q</td>
</tr>
<tr>
<td><strong>Twinning</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contracting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disbursement</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Contract 2 – Supply</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contracting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disbursement</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Commission for Personal Data Protection

Needs Assessment
Technical Specification

Date: 19.07.2005

1 INTRODUCTION
1.1 Purpose of this document
The overall objective of this document is to describe the main characteristics of the software required for Commission for Personal Data Protection, to suggest a possible framework for the development of the software and to assist in the identification of the requirements necessary for the successful implementation of the software in the testing/training environment and in the Commission environment (proof of the full functionality). Also the hardware required for countrywide roll-out of the software is specified in this document.

The specific objectives of this document are to suggest a:

- Definition of the scope, objectives and phases of the equipment component,
- Definition of the functional and technical requirements,
- Definition of the technical approach,
- Definition of the activities and tasks to be carried out,
- Description of the overall management and methodological approach,
- Indication of timescales and rough estimation of resource requirements.

1.2 Abbreviations and acronyms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMMISSION</td>
<td>Commission for Personal Data protection</td>
</tr>
<tr>
<td>BENEFICIARY</td>
<td>Commission</td>
</tr>
<tr>
<td>IS</td>
<td>Information Systems for the Commission</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
</tbody>
</table>

2 SCOPE OF THE PROJECT
2.1 Overview
Existing IT resources:

Computers at CPDP are 32. They are 3 types with following characteristics:

**HPCompaq - 16 number:**
- CPU: Intel P4 2.66GHz
- RAM: 256MB
- HDD: 40 GB
- Monitor: HP1702 17” LCD
- Licenses: Microsoft Windows XP Professional, Microsoft Office XP Professional

**DELL - 10 number:**
- CPU: Intel Celeron 2.00GHz
- RAM: 256MB
The goal of the project is to provide an automated, web-based, centralized, scalable, secure and reliable information system for the needs of the Commission.

A successful countrywide roll-out of the IT application in Commission strongly depends on the network (WAN and LANs) and the hardware (servers, workstations etc.) available at the Regional Units. Therefore, it is the obligation of the Beneficiary to secure the minimum technical environment as far as it is not contained in this tender to be installed in due time.

### 2.2 Summary requirements and deliverables

The equipment components are as follows:
- Software (standard and application);
- Hardware;

*The scope of the project suggests division in lots to give the tenderers opportunity to supply deliverables according to their expertise. It is usually known that companies specialized in hardware are not obligatory perfect in software and vice versa. However separated Lots would afford the best available tenderers to be selected.*

The main requirements of the Software component are to:
- Start and implement a project covering the expected results mentioned above, which shall include the following main steps:
  - Evaluate the needs and requirements (*no existing systems*)
  - Plan, design, provide and test an IS, according to ch. 3
  - Perform the final acceptance test of the full functionality of the system in the testing / training environment at the Central Unit
  - Perform the final acceptance test of the full functionality of the system in the Commission environment *(country-wide)*
  - Deploy the system countrywide *(roll-out)*

  Provide user training in close co-operation with the Commission experts

The main requirements of the Hardware component are to:
- Provide the (additional) hardware needed as specified under ch. 4

The deliverables for the equipment component (software) will follow the Unified Development Process (UDP) Standards and Guidelines.

### 3. APPLICATION AND STANDARD SOFTWARE

#### 3.1. FUNCTIONAL REQUIREMENTS TO THE APPLICATION SOFTWARE

**Business environment**

Structure of the Commission for Personal Data Protection:

The Commission for Personal Data Protection consists of a Central Unit and 6 Regional units.
The commission should register all applications and related documents connected with the personal data handling of different organizations and concerned persons. The commission creates statistical reports and analysis concerning the personal data handling.

Users of the IS are as follows:

- members of the competent departments working on personal data at the Central unit
- members of the 6 Regional units

**Existing IT applications in the Commission for Protection of Personal Data**

N/A

**Goals and expected results**

*Optimization of the work of the commission; Optimization of the processes; Cost Effectiveness*

**Functional requirements to the application software**

In order to achieve the goals the following functions have to be realised by the contractor:

- **Data entry** functions
- **Workflow** functions
- **Query**
- **Statistic** functions and analysis
- Daily weekly and monthly **bulletins**

The following results shall be achieved with these functions:

*Shortening of the duration of proceedings; Saving of costs; Better information management and access.*

**Data entry functions for the Central Unit**

Process for entering, registration and other initial activities (document scanning and indexing).

**Data entry functions for the Regional Unit**

Process for entering, registration and other initial activities (document scanning and indexing).

**Workflow Functions**

Processes for approvals, rejection, complains etc. with corresponding level of automation – auto-reminders, graphical process definitions, access management, etc.

**Statistical functions**

To meet the requirements of the Commission, additional daily, weekly and monthly statistical evaluations and analysis are necessary.

**3.2. TECHNICAL REQUIREMENTS TO THE APPLICATION SOFTWARE**

**3.2.1 Communication requirements**

The system will operate as a countrywide application with Web based interface. The communication therefore is a main requirement for the successful operation of the system. Following criteria have to be fulfilled to establish the connectivity within the different units and at the central unit:
LAN at Regional units: All users, working with the system, have to be connected to the local area network. These networks must be established in the regional units and must be capable of supporting the transactions volumes generated by the application.
LAN at the Central unit: The application and database servers will be established at the central unit.

Communication between the regional and central units: The WAN within the Commission network of the republic of Bulgaria has to guarantee the data-transaction between each regional unit and the central level.
The security of those country-wide connections has to be ensured. Adequate equipment for network-security has to be installed.

3.2.2 Minimum Hardware requirements
The application will be a centralised system. The system should be able to operate on the minimum hardware configuration in accordance with the requirements below.
The general minimum hardware requirements:
- Data Base at central level - 2 Data Base Servers, 4 way 64-bit Processors
- Data Base for Public Access – based on the 4 way Xeon Processors
- Applications Server Farm (Servers for Public Access, Servers for Internal applications, Backup/Archive server, etc.) – Blade technology with 2-way, 4-way blades mixed enviroment
- SAN Infrastructure (Switches, cabling, etc.)
- SAN Storage at least 2,4TB in RAID10, upgradable to 60TB, min 32 partitions, flash copy, etc.
- Tape Library with FC interface
- Racking and options
- Workstations

To achieve maximum scalability and future growth of data, the servers must be connected to SAN.
All equipment has to operate at 220-230 Volt, 50 Hertz power supply. All equipment shall conform to the applicable technical regulations of the EU (CE marking; Safety, EMC, etc.).

Software Requirements to the application software
General requirements
Achieve a high degree of user-friendliness and ease of use: consistent screen design, graphical icons, data entry assistance and validation, help screens, etc.
The system design must allow further enhancements and changes.
The system must operate in clustered environment to maximise the fault protection.
The application has to be developed in respect to PKI security model.
The security model must ensure data access to entitled users and user-groups in respect to their roles and functions. This includes a full range of access levels for different functional users. This should allow an administrator team to register/remove/change users and their access levels. The system should allow designated officers to manage passwords, authorisation etc. The security model has to ensure, that the administrative effort is minimised.
The application should provide functionality for automatic indexing of scanned different paper forms and documents.
The application should provide an interface for building automating indexing processes over scanned documents without need of any additional software development.
The system should include workflow capabilities, including document routing with decision points, actions, action lists, parallel routing and custom script support. The workflow functions should have graphical builder within to enable non-technical users to easily define document routing processes.

The documentation shall include: user manuals, function user guides, administrative guide.

The system should be (platform-) independent.

**REQUIRED BUSINESS APPLICATION FUNCTIONS**

Archiving: for backup and balancing workload of application.
Backup and Recovery: System must be recoverable from crash within 1/2 workday.
Query functions via the internet: so that the parties involved in the process and other authorized administrations interested in a proceeding can inform themselves at any time about new proceedings as well as about the current status quo of the organisations.
Statistic functions for the drawing up of the statistical reports.
Document management: full history for document access and changes.

**REQUIRED TECHNICAL APPLICATION FUNCTIONS**

Consistent screen design, graphical icons, data entry assistance and validation, help screens, etc.
The system design must allow for further enhancements and changes.
User management functions: for managing the application users.
Integrated system: integrity of data should be checked, monitored, controlled and managed.
Data capture once at source: data will be entered once and once only and validated and verified at the source point in the business process. This will ensure data integrity is maintained throughout the system.

The system must be fully password protected, including network and systems protection where appropriate. Security must be user oriented as well as data or function execution oriented. In any case the password facility must be capable of assigning simple or combined privileges based on:

- Display Screens, (permission: view)
- Menus, (permissions: view, execute)
- Display Screen Fields, (permissions: view, change)
- Reports (permissions: create, view, print)
- Execute procedures, functions etc.
- Read data
- Add data
- Delete data
- Change data
- Field level security

Printing functions: print locally or centrally, create automatically notes, notifications, statistical information, lists, and results of queries.
The system should support both manual and automatic register actions.
Dossier tracking system: The status quo of a organisations dossier should be precisely and easily monitored at any time. Statistical information can be obtained on local and central levels.
Search: full-text searching capabilities.
E-mail event notifications.
Registration and processing of requests from outside organizations and authorities – via web request form.
Import / Export features: will include the ability to import, export and manage various file formats including; objects (.bmp, .gif, .jpeg, etc.), photographic images, Emails, scanned docs etc.

Functions:
• Data entry, repository and processing of information.
• Issuing of documents for different organizations
• To create reports, necessary for different organizations and authorities.
• To create statistical reports according to specified criteria.

REQUIRED SECURITY APPLICATION FUNCTIONS

The system must ensure data access to entitled users and user-groups in respect to their roles and functions. This includes a full range of access levels for different functional users.

The system should provide managing of user roles and access levels to be performed by non-technical users.

The system should provide DB security.

The system should provide intrusion detection handling; detect, register and alert on any attempt of not authorized access or suspicious activities.

The system must provide all the standard security features: username/password authentication of the users and flexible rights management.

The system should propose special user level security and audit sub-system.

The system should propose management of the privileges of different user groups. It should be possible to grant appropriate rights to the users directly and to a group of users as well.

Level access protection should be possible.

The potential for unauthorised external or internal access must be minimised. Data must be protected by a combination of system and clerical procedures incorporating security features

The system should monitor all access by users and provide a comprehensive audit trail.

The system must be fully password protected, including network and systems protection where appropriate. Security must be user oriented as well as data or function execution oriented. In any case the password facility must be multilevel (at least two-level), embedded, and be capable of assigning simple or combined privileges based on:
• Display Screens, (permission: view)
• Menus, (permissions: view, execute)
• Reports (permissions: create, view, and print)
• Execute procedures, functions etc.
• Read data
• Add data
• Delete data
• Change data
• Edit data

The system should provide hierarchical levels of access.

System must provide field level security.

The back-up and security features must be capable of being used by non-technical personnel.

The ‘back-up’ and restore procedures must be automated and supported with user manuals and training.

The system requires programme protection to prevent:
• Accidental/occasional programme or data damage by non-qualified users
• Intentional programme or data damage;
• Unauthorized copying and distribution of sensitive information;
The security of country-wide connections has to be ensured. Adequate equipment for network-security has to be installed. The use of private line (Intranet) reduces the number of systems exposed to the Internet compared to a VPN solution.

**REQUIRED NETWORK APPLICATION FUNCTIONS**

Application must support XML data interchange;  
Support of remote administration;  
Application must support replication;  
Application must support collaboration services;  
Data flow and all transactions must be encrypted.

The system should provide single sign-on. Users must be authenticated to the system by username and password and then they must have access to all system and network resources without entering username and password again.

**Principle architecture**

The architecture will be centralised Web-based, multiplatform system and must conform with the open industry standards.

At the Commission central unit will consolidate all data. This central level will provide the service for all statistical queries and the place for public information.

There are 6 Regional units. Each regional unit must have a connection to the central server via WAN.

The whole system consisting of hardware, connectivity and applications has to fit together. The public accessed servers should be separated from the main database servers.

1. **RDBMS FUNCTIONALITY GLOBAL REQUIREMENTS**

1.1. **General requirements:**

1.1.1. The automated approach should consist of base and public DB; the base DB must be replicated (chosen information) in the public DB.

1.1.2. The Application SW provides search possibilities, according to different characteristics and criteria. The time for search should not exceed 1 min.

1.1.3. RDBMS must conform the ANSI SQL-92 standard.

1.1.4. RDBMS must be platform independent

1.1.5. The Supplier of RDBMS must propose at least 1 (one year) licensing warranty for new versions and updates

1.1.6. RDBMS must support minimum 4 CPUs per server

1.1.7. RDBMS must have multi-instance support, enabling multiple, isolated installations of RDBMS on a single server

1.1.8. RDBMS must support database size greater than 2 GB

1.2. **Management tools**

1.2.1. the RDBMS vendor should also provide a GUI tool or set of tools, enabling faster and easier database management. Command line management tools however should be also available, for executing management scripts in batch mode and ensure ring better control

1.2.2. RDBMS must have the functionality including but not limited to: perform database backup and restore remotely; create, alter, and script all database objects including stored procedures, triggers, and views; create and schedule database
jobs; object search/filtering based on code content or object name; index
rebuilding and database fine-tuning; query window for running queries and
editing data;

1.2.3. User errors protection - often the most harmful problems arise when user
accidentally damages data (deletes or updates wrong data). The RDBMS should
be able to flash back in time and query the data in the way they have been
specified time ago, within predefined time frame. This will enable creation of
self-service error correction procedures, without ant system downtime.

1.2.4. Partitioning - due to the hard management of the very large tables, the RDBMS
should have an efficient partitioning functionality. The tenderer shall describe the
features of the partitioning of the RDBMS and the underlying algorithms used

1.2.5. RDBMS must have auto-tuning and auto-management functions to automate
database administrator tasks.

1.3. Security

1.3.1. RDBMS must have implemented auditing rules allowing tracking successful
and failed use of permissions when accessing individual database objects. The
audit information must contain the timestamp, identifier of the account that
triggered the event, target server name, event type, its outcome (success or
failure), name of the user's application, and Server process id of the user's
connection.

1.4. Data Access

1.4.1. For the purposes of integration RDBMS must support connectivity to
databases of major RDBMS vendors and to, but not limited to, OLE DB and
ODBC.

4. HARDWARE SUPPLY

Hardware to be offered:
- Data Base at central level - 2 Data Base Servers, 4 way 64-bit Processors
- Applications Server Farm (Servers for Public Access, Servers for Internal applications,
  Backup/Archive server, etc.) – Blade technology with 2-way, 4-way blades mixed
  enviroment
- SAN Infrastructure (Switches, cabling, etc.)
- SAN Storage at least 2,4TB in RAID10, upgradable to 60TB, min 32 partitions, flash
copy, etc.
- Tape Library with FC interface
- Racking and options
- Workstations

Data Processing Center:

Main database cluster

Servers minimum requirements:
- 4-x 64 bit RISC processors, upgradeable to min 16 processors
- 16 GB Memory, ECC, upgradeable to min 64 GB
- 2x 100/1000Mb Ethernet LAN attachment
- 2x FC Adapters
- Redundant power supply

Cluster management software
For the SAN:
Minimum requirements:
• 4,8 TB raw disk storage (upgradable min 60TB)
• High availability design
• Min 32 logical subsystems
• Multipath support
• Flash copy support

SAN Infrastructure:
2x16Port SAN Switches (zoning support), cabling, etc.

Applications Server Farm:
Blade technology with full redundancy (networking, fiber-channel, power supplies, etc.)
Internal applications servers: 2x Xeon blades, 4 GB RAM, FCA
Public applications servers: 4 x Xeon blades, 8 GB RAM. FCA
Public Database server: 4 x Xeon blade, 8 GB RAM, FCA
Backup server: 1xXeon blade, FCA

For the Backup solution (Tape Library): Devices to backup the data of the servers. Depending on vendor specific features of possible hardware configurations, the supplier may offer a hardware and software in accordance with the requirements. The FC interface for direct attach to SAN is a must.

For the workstations:
Minimum requirements:
• Processor: Pentium IV 2.4 GHz
• Memory: 256 MB DDR
• Internal Disk Drives: 40 GB ATA 100
• Removable media drives: 48x CD
• Video Card: 32 MB Ram AGP4x 1024x768x85 Hz
• LAN adapters: 10/100Base T LAN with RJ45 connector
• Operating systems: W/O
• Monitor: 17” TCO’ 99

All performance and security etc. related aspects have to be satisfied by the suggested hardware architecture.

Warranty period for the hardware
It is required that all equipment and facilities supplied through the project will be maintained by the supplier for 36 months from the date of the delivery acceptance protocol.
• the preventative hardware maintenance and software update schedule,
• a list of the spare parts and replacement units which are expected to be held on-site,
• proposed local maintenance and support capacity,
• how an effective “hot line telephone and support desk” service will be established.
Building a local national network of CPDP on the territory of the Republic of Bulgaria

1. Technical Solution
   a. General description
   The current technical solution observes the development and the implementation of the local network infrastructure in the campus of Agency for preventing of the personal information. The main purpose of the technical solution is to offer network infrastructure, which is able to meet the company’s requirements for number of users, network traffic for general purposes and special applications, reliability, flexibility, good performance and security. In the project is paid special attention of the opportunity for future growing of users’ number, used network services, and increased network traffic. To increase the company security and keep the confidentiality of the data is recommended an improved network infrastructure of the internal and external security system.

   The offered infrastructure is with a hierarchical model. The network is separated on levels, which allow easy maintenance and great scalability without redesign of the rest of the network structure. The both main levels are: Enterprise Campus – describes the internal network infrastructure into the headquarter of the company and Enterprise Edge – describes the whole strategy for building the corporate security and the system for remote connections, as well as the whole network equipment for security and termination of remote security connections, installed into the central office of the company (Fig. 1).

   Enterprise Campus has hierarchical structure and is divided into the following sublevels: Core - Distribution Level and Access Level. Core - Distribution Level build the foundations of the logical center of the local network. It is build with fast switching devices with integrated functionality for network redundancy of the L2/L3 infrastructure, which is connected with high bandwidth transport links. To Core - Distribution Level are attached the following levels and modules:

   - Sever Farm module
   - Management module,
   - Main Enterprise Edge level
   - Access Level.

   The separating of the logical center – Core - Distribution Level gives the following advantages of the end user into the local network infrastructure:

   - Increase the throughput for access to shared services and applications.
• Decrease the time necessary of the end user for access to the offered services.
• Provides fast transportation of data into and outside of the network.
• Offer 100% availability of the resources and unlimited opportunities for future growing.

Access Level connects the end users to the network. On Access Level is given possibility for dividing the users in separate user groups (VLAN). The dividing into VLAN allows control of the traffic and opportunity to apply company policies for user access (authentication and authorization) for the end users (company staff). To Core - Distribution Level does not pass traffic, which is local for a user group.

Enterprise Edge is used for:
• Gives opportunity for connections with the remote and branch offices of the company (existing and future) to the Server Farm module and the users, who connects to the local network from the Access Level into the central office of the company.
• Connection to the public Internet to use its resources and services.
• Gives access to public information of the company.
• Gives access on partners and information and resource providers without any security content that are allowed for public use.
• Gives access of remote users (staff, who is out of office for any times) to resources that are on the Server Farm модула и Access Level into the central office of the company.

On that level is installed equipment that establish a connection with the WAN network and build the external network security of the company.
The network security for access of external users (Remote Offices and Users) is provided on Enterprise Edge level. The connections with the remote offices are established through VPN network over the existing public Internet (Fig. 2). The VPN network guarantees security of the transported data from remote and branch offices to the central office. The recommended VPN topology is star. Another opportunity to create the same structure is the using of leased lines, but VPN has the following advantages over the structure with leased lines between the offices of the company:

- **VPN** offers lower price than leased lines. The price to establish VPN network is decreased by the low price to transport the traffic, because there is no more need of the backbone equipment and services. The price of LAN-to-LAN connection realized with VPN usually reduces the price with 20 to 40% compared with leased lines.
- **VPN** offers flexibility to achieve economy of the Internet connection. VPN is more flexible and scalable network architecture than the general WAN networks, build with leased lines. As well the company could quickly and efficiently add new and/or remove existing connections depending of the business requirements.
- **VPN** network offers easier maintenance than the owning of private WAN network, based on leased lines.
With VPN network, the users in the remote offices have advantages when they transmit data:

- Confidentiality (encryption) – The sender encrypt the information before transmit it through the public network. The encryption is done invisible for the end user. With adding encryption on the data, nobody could read the data, except the receiver of the data.
- Data integrity – The receiver could check, whether the received data from Internet are whole and unchanged.
- Origin authentication – The receiver could check the source of the information (identity of the sender).

The using of VPN allows on the staff of the company to access the company’s resources with building a VPN tunnel from everywhere, where there is access to the public Internet. A VPN tunnel is established only if the user is authenticated which allows him to use the network infrastructure. The both sides of a VPN tunnel should be configured in the same way (encryption, IKE).

b. **LAN**
   
i. **Infrastructure**
This section offers a real solution for *Enterprise Campus* from the network infrastructure based on the previous section. Based on the previous segmentation, the network levels are divided on four network modules:

- **Core & Distribution Level** – provides the core communication with backup connections and optimizes the use of the main network resources as resilient aggregated links, switch stacking and the common management of the distributed L2/L3 switching factories in that network module. The used distribution switches are connected into a stack, which provides tools for distribution on the switch factories on L3 and switching DB on the L2 technology.

- **Access Level** – provides access points for the end users to all authorized levels of the network infrastructure. On that level the users could be grouped based on signs that are regulated from the company such as department, location of the building and etc. The separated switches could connect with *LACP – Link Aggregation Control Protocol* to the core switches. LACP protocol has two main advantages:
  
  - The grouping of several physical interfaces into one logical interface, whose bandwidth is the sum of the bandwidths of the physical interfaces.
  - The set of links grouped into a logical interface are reserved each other and the link between the connected devices.

- **Server Farm** – provides high speed and uninterrupted connection on the server farm to *Core & Distribution Level*. The current network solution is connected to the core switches with two connections, on which is enabled *LACP – Link Aggregation Control Protocol*, which provides higher bandwidth and redundancy for the server connections (Fig. 3). The using of *LACP* allows sharing of the traffic between the both aggregated links increases the available bandwidth almost twice for the links to the servers.
Management Module – provides the following functionality for the network infrastructure:

- **Fault Management** – determines, isolates and alerts for occurred problems into the network infrastructure.
- **Configuration Management** – collects and stores the configuration of the network devices.
- **Performance Management** – collects information for the load of the network links and devices.
- **Security Management** – restricts the access to the network devices and resources.

The Management module is a part of the system, which allows full administration of the whole network infrastructure from. We could collect and estimate information for the network equipment. The collected information is used to follow the necessity of changes that we have to do when we add new users and/or add new services such as VoIP or video conference systems.

Layer 2 connectivity between the separated switches:
As it was described in the previous section **Core & Distribution Level** we offer two distribution switches connected into a stack, which work as one unit. This approach allows full redundancy of the core infrastructure of the company. If one of the core switches fails or is stopped for tests, the other one continues to maintain the connection between the rest modules and levels of the network infrastructure (**Server Farm module, Management module, Access Level & Enterprise Edge**). By this way we increase the availability of the network infrastructure and reduce the time, in which the users could not use the resources (Downtime of the network infrastructure). We offer to establish aggregated links between every access switch with the both distribution switch. By this way access switches are connected with one copper link with available bandwidth 1 Gb to every core switch. The copper links from the **Access Level** to the core switches are going to be managed with **LACP – Link Aggregation Control Protocol** and they will work as one logical link with higher bandwidth. This means, that the connectivity on the **Access Level** switch to the core switches has almost 2 Gb per second. If one of the both connections fails, the access switch still has a connection to the rest modules of the network infrastructure. The time for synchronization is low if a connection fails.

**ii. Supported protocols**

1. **Level 2 Protocols** – to provide optimal connection between the components in the network infrastructure and between the different levels and modules is necessary and enough all devices to support **LACP–Link Aggregation Control Protocol**. LACP gives opportunity to build completely reduced solutions on all levels of the network infrastructure. **RSTP – Rapid Spanning Tree Protocol** allows backup of the main link to the core network infrastructure. To segment the first offered network infrastructure and to separate it on a few **VLANs**, is necessary all devices to support **VLANs** with marked (colored) packets – **tagged VLAN** – 802.1q and port based **VLANs**.

2. **Level 3 and 4 protocols** – as basic transport protocol on level 3 are used the IP protocols. For normal routing on **VLANs** are necessary **L3** switches in stack mode to support static routes and dynamic routing protocols such as – **RIP** and/or **OSPF**.

**c. WAN**

1. **Infrastructure**

   **i. Protection from connection failures on the connections with the remote offices**

   The **WAN** infrastructure envelops the periphery on the **Enterprise Edge** module. The connection to the central office of the company to the Internet is going to be
established through two Internet providers. (Fig. 4). The central office of the company is going to be accessible from both Internet providers in the same way. To achieve full redundancy goal we will think for our network as Autonomous System (AS3) that connect to two other AS on the Internet providers as a full meshed network topology. (Fig.4).

**How does it work?:** The central office, assigned to AS 3 (Central Office), has two connections to Internet through Internet service providers AS 1 and AS 2. The connection to the remote office through the Internet provider AS 1 is used as primary (Remote Office → Internet provider AS 1 → Central Office AS3) and the secondary connection through Internet provider AS 2 is a backup in case the primary connection fails (Remote Office → Internet provider AS 2 → Central Office AS3). It is shown on Fig. 4 (Case 1). The firewall into the remote office checks whether the primary connection is active and it transports traffic, through sending a set of small packets on scheduled time intervals (they consume very small amount of network resources). If the primary connection fails, the system waits a defined period of time (defined from the client and it is usually 20÷40 sec), during which is possible the primary connection to restore her proper functionality. If the primary link continues to be down, the remote office firewall establishes a connection marked with Case 3 on Figure 4 (Remote Office → Internet provider AS 2 → Internet provider AS 1 → Central Office AS3). If a connection between Internet provider AS 2 and Central Office AS 3 fails, the primary connection is not restored between the remote office and Internet provider AS 1, but exist a link between Internet provider AS 1 and AS 3, the connection will be restored by the followed way: Remote Office → Internet provider AS 2 → Internet provider AS 1 → Central Office. It is shown on Figure 4 with Case 2.
Fundamental question is the requirement for connection between the both Internet providers AS 1 and 2.

2. **Building a security connection to the remote offices**
The building of a secure connection, as we have already mentioned, is going to be achieved with a network based on VPN tunnels which is shown on the next schema. The identification of the tunnels is going to be done with X.509 certificates, issued as child certificates from a certificate which is issued from a company that have a license to do it such as Verisign and etc.

![Central Office Diagram]

Every remote office has issued own certificate, which is separated in two parts. One of the parts is installed into the remote office, the other one is installed into the central office.

The central office owns the root certificate (issued from the licensed company such as Verisign).

![Supported Protocols Diagram]

**ii. Supported protocols**

1. **Level 2 protocols** – to provide communication in the modern heterogeneous WAN networks is necessary to use various transport synchronous/asynchronous network protocols such as PPP, HDLC, Frame Relay, and X.25.
2. **Level 3 and 4 protocols** – as basic transport protocol on level 3 are used the IP protocols. For normal routing between the AS is necessary the routers to support static routes and dynamic routing protocols such as BGP. To establish security communication links with high level of security and performance are used IPSec with DES/3DES, RSA and etc.

d. **DMZ**

DMZ is a special part of the network structure of the Enterprise Edge, where are separated the servers for public access. Specific settings, depending of the client requirements are deployed on the firewalls for DMZ. The shown on the next Figure 6 schema is designed with failover of the links, which guarantees high availability of the system.

The servers are connected to the both core switches with links on 100 Mb / Full Duplex. The both switches work as one unit under common control – stack mode, which allows resilient links with the servers. We need of the “stack mode”, because of the opportunity to use LACP protocol to bundle the links in on logical link. To configure the stack mode on the switches are installed Cascade Stacking Kit. The ports, connected to the both firewalls are set to STP.
enabled. On all of the rest ports that are connected to the servers, the STP is disabled, which allows them to jump from blocking state to forwarding state without the normal delay. The both firewalls work in mode Active / Passive – one of the firewalls is always in standby mode and could replace the other one if it fails. To set up for that mode of work between the both firewalls is added a connection. The both switches have a double connection with every firewall, but one of them is active and one is blocked from the STP.

**e. Remote Office Infrastructure Design**

The remote offices are designed with the structure shown on figure 8. The firewall is used to terminate the VPN tunnel to a remote office and to guarantee the security access of the end users to Internet. The connection with Internet is made resilient to two Internet providers. The users into the remote office are attached to a common switch on which is added a system for control of every port with 802.1x and a RADIUS server (figure 7). When the access of the computer is allowed to the switch ports, the users could use the network resources when they authenticate on the Domain Controller.

To remote offices are connected not more than N small Branch Offices, which have only a few computers in it. Their infrastructure includes a firewall to establish a VPN tunnel and the connection to the Internet is not redundant. The
f. **Security**

i. **Infrastructure**

The security plan into the network infrastructure could be separated on two parts:

1. **LAN security**

In this approach of the policy of the security, a main problem is the management of the users’ access to the network resources into the company. It is necessary to support mechanisms which control the behavior of the users when they login into the domain of the company on network level. In that case we deploy protocol for authentications and control of the access 802.1x, which is embedded into the switches, offered as *Access Level* devices. This model for control of the access works successfully with RADIUS servers produced by Funk Software or Microsoft. Our preferences to realize that solution are to the Funk software products, because of the better opportunities for scalability and supported many different scenarios and schemas for control of the access. The logical schema of authentication is shown on fig. 8.

The user’s computer has not any access to the network, before it authenticates on the RADIUS server. On the first step the user sends a query to the switch port, which redirects the query to the RADIUS server. All other packets will be dropped until the user is successfully authenticated. If the RADIUS server allows access of the user’s computer, the port of the switch, on which it is connected, is unblocked and starts to transport the user’s computer traffic (Step 2). The advantage of the RADIUS server is the opportunity to control the access, which the users have.

2. **Perimeter Security and VPN Termination**

The focus when creating a strategy for security on the border of the network infrastructure falls over the right selection,
installation and configuration of the firewall system, which includes the next components:

- A set of one or more hardware devices, united into a appropriate schema to achieve full redundancy to the core switches
- Software for management and configuration of the firewall
- Analyses of the retries of hacks tried from the gateway for public connections
- Tools to terminate the remote encrypted channels, initiated from the gateways of the remote offices that have tunnels properties or mobile users that have tunnel properties
- Integrated system for anti-virus protection
- Tools for analyses on the whole infrastructure of the security on LAN and WAN.

**ii. Supported protocols**

1. **Level 2 protocols** – to provide the communication into the internal office is necessary to support a variety of Ethernet protocols over copper cables.

2. **Level 3 and 4 protocols** – as basic transport protocol on level 3 are used the IP protocols. For normal routing between the AS is necessary the routers to support static routes and dynamic routing protocols such as BGP. To establish security communication links with high level of security and performance are used IPSec with DES/3DES, RSA and etc.

**g. IP Telephones**

1. **Description**

   Into the current design of the network infrastructure is kept place for VoIP. On figure 9 is shown, how the VoIP is going to be implemented into the VPN network. The offered schema is topology star.
ii. **Supported Protocols** – H.323, G.711, G.729a/b, ADPCM, 802.1d, 802.1p, 802.1q, 802.2, 802.3, 802.3af, 802.11, IP, IP-ToS, DiffServ, TCP/IP, UDP/IP, DHCP, DNS

ANNEX 6


2. Rules for the activities of the Commission for Personal Data Protection and its administration enforced since 31.01.2003 issued and promulgated in the State Gazette.

3. Law for the Ministry of the Interior

4. Law for the Civil Registration
# ANNEX 7

## INDICATIVE LIST OF EQUIPMENT

### 1. Training Centre of CPDP

<table>
<thead>
<tr>
<th>Justification</th>
<th>Available equipment</th>
<th>Necessary equipment</th>
</tr>
</thead>
</table>
| Establishment of a CPDP centre for training external personal data controllers and the CPDP administration | | ▪ 25 x PCs  
▪ 2 x Servers  
▪ Powerful LaserJet Printer  
▪ Shredder  
▪ Colour LaserJet printer  
▪ Flat Scanner A3  
▪ Operating systems (e.g. Windows XP Pro, Win2003 server etc.)  
▪ MS Office 2003 Pro  
▪ Powerful Multimedia Device  
▪ 2 x LAN Switch, 16 ports |
2. Information system of CPDP

<table>
<thead>
<tr>
<th>Justification</th>
<th>Available equipment</th>
<th>Necessary equipment</th>
</tr>
</thead>
</table>
| CPDP is building up an information system for the register of the controllers of personal data. | **Computers** at CPDP are 32. They are 3 types with following characteristics:  
- **HPCompaq - 16 number:**  
  - CPU: Intel P4 2.66GHz  
  - RAM: 256MB  
  - HDD: 40 GB  
  - Monitor: HP1702 17” LCD  
  - Licenses: Microsoft Windows XP Professional, Microsoft Office XP Professional  
- **DELL - 10 number:**  
  - CPU: Intel Celeron 2.00GHz  
  - RAM: 256MB  
  - HDD: 30 GB  
  - Monitor: DELL 17” LCD  
  - Licenses: Microsoft Windows XP Professional, Microsoft Office XP Professional  
- **LAPTOPS:**  
  - **HPOmniBook - 6 number:**  
    - CPU: Intel P M 1.8 GHz  
    - RAM: 256MB  
    - HDD: 40 GB  
    - Monitor: 15” LCD  
    - Licenses: Microsoft Windows XP Professional, Microsoft Office XP Professional | **Hardware to be offered:**  
- Data Base at central level - 2 Data Base Servers, 4 way 64-bit Processors  
- Applications Server Farm (Servers for Public Access, Servers for Internal applications, Backup/Archive server, etc.) – Blade technology with 2-way, 4-way blades mixed enviroment  
- SAN Infrastructure (Switches, cabling, etc.)  
- SAN Storage at least 2,4TB in RAID10, upgradeable to 60TB, min 32 partitions, flash copy, etc.  
- Tape Library with FC interface  
- Racking and options  
- Workstations  
- Data Processing Center:  
  **Main database cluster**  
  Servers minimum requirements:  
  - 4-x 64 bit RISC processors, upgradeable to min 16 processors  
  - 16 GB Memory, ECC, upgradeable to min 64 GB  
  - 2x 100/1000Mb Ethernet LAN attachment  
  - 2x FC Adapters  
  - Redundant power supply  
  - Cluster management software  
- **For the SAN:**  
  Minimum requirements:  
  - 4,8 TB raw disk storage (upgradeable min 60TB)  
    - High availability design  
    - Min 32 logical subsystems  
    - Multipath support  
    - Flash copy support  
  **SAN Infrastructure:**  
  2x16Port SAN Switches (zoning support), cabling, etc.  
  **Applications Server Farm:**  
  Blade technology with full redundancy (networking, fiber-channel, power supplies, etc.)  
  Internal applications servers: 2x Xeon blades, 4 GB RAM, FCA  
  Public applications servers: 4 x
**3. Countrywide network of CPDP**

<table>
<thead>
<tr>
<th>Justification</th>
<th>Available equipment</th>
<th>Necessary equipment</th>
</tr>
</thead>
</table>
| - CPDP is building up a countrywide network for its administration. | 1. LAN  
Access Level  
5 x Switch 28-Port  
10x 1000Base T SFP  
Core-Distribution Level  
2 x Switch 24 Port  
1 x Switch Resilient Cable  
2 x Switch Stack Cable  
Server Farm  
1 x Switch 24 Port  
DMZ  
2 x Switch - 24 x 10/100 BaseT + 4 SFP, enhanced software image  
1 x Switch Resilient Cable  
Enterprise Edge  
1 x Router, 8 MIM slots |
| Router 2 Port 10/100BASE-T MIM module | 2 x Router 2 Port 10/100BASE-T MIM module  
| 1 x Router  2-port Sync/Async MIM with x.21 | 1 x Router  2-port Sync/Async MIM with x.21 |
| Necessary approximated costs (EURO) | 80 000 |

2. Firewall
Core Office
1 x Firewall
Remote Office
6 x Firewall

Necessary approximated costs (EURO) 30 000

3. VoIP
Core Office
1x IP Telephony Solution with the necessary components
1 x UPS – 5 KVA
Remote office
6x  IP Telephony Solution with the necessary components
6 x UPS – 5 KVA

Necessary approximated costs (EURO) 40 000

approximated costs (EURO) 150 000