



[www.ddsi.org](http://www.ddsi.org)

## National Dependability Policy Environments

### SLOVENIA

Report Version: Final  
Report Preparation Date: 1 November 2002  
Classification: Public  
Preparation led by: Almaweb (I)

Contract Start Date: 1 June 2001      Duration: 18 months  
Project Co-ordinator: RAND Europe (NL)

Partner: RAND Europe (NL, Project Coordinator); King's College London (UK);  
Cell Network (S); IABG (D); Almaweb (I); LINK (P); ELIAMEP (GR);  
Ernst Basler + Partner (CH), Isdefe (E)



IST-2000-29202

Project funded by the European Community  
under the “Information Society Technology”  
Programme (1998-2002)

**Table of Contents**

Overview of the Country’s Information Infrastructure ..... 3  
Main ICT Regulatory and Legal Developments ..... 4  
Assessment of Phenomena Undermining Dependability ..... 6  
Government Initiatives Aimed at Tackling Cyber-Security ..... 7

### ***Overview of the Country's Information Infrastructure***

Slovenia has enthusiastically embraced the opportunities offered by ICT and e-commerce. The most visible symbol is the creation of a specific Ministry for Information Society (MID), an expression of the political will to provide a government-led stimulus to change, speed up transformations and to offer their benefit to the widest number of citizens. The MID is preparing a State programme for e-Slovenia.

The functions of the Ministry are to bring together under a single roof the two previously largely unconnected areas of telecommunications and development of an e-society; and to provide a coherent framework, within the eEurope+ concept, to a number of uncoordinated e-initiatives and e-policies, both private and public. Other functions are to draft and pass a Strategy for e-Government with the aim of introducing e-administrative procedures and enabling e-services to citizens; and to provide political guidance to the CVI (Government Centre for Informatics), while supervising the harmonisation of Slovenian telecommunications with the *acquis communautaire* of the EU.

The Ministry itself operates in a particular political and organisational framework. Above the Ministry and directly created by the Prime Minister, is the Council for Information Society, which is tasked with the provision of the strategic guidelines for the whole ICT modernisation and harmonisation process.

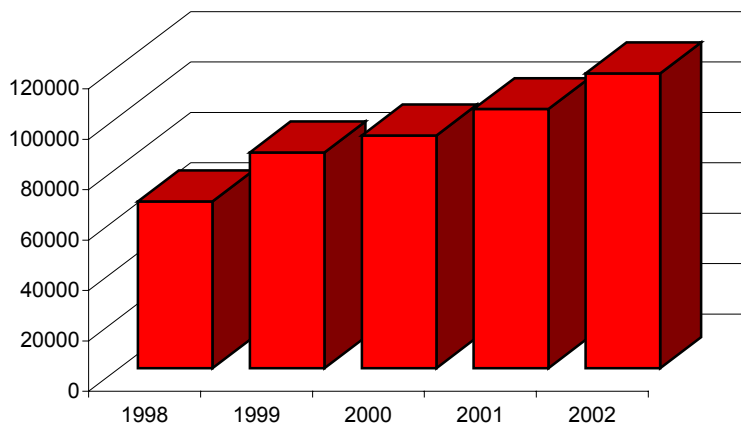
Within the structure of the government, the Commission for Informatics for the Field of Public Administration, a working body responsible for the 'informatisation' and establishment of e-commerce practices within the public administration, operates. Its functions are to monitor, discuss and evaluate both legislative and operational projects, while co-ordinating tasks assigned by the government to different state bodies in this field.

Under the responsibility of the MDI, the CVI functions and, in addition to its other planning and co-ordination tasks, it is also responsible for the drafting of the annual harmonised plan of informatisation. The CVI also plays an essential role in evaluating and co-ordinating both the needs and the procurement of different public bodies. In several instances it can, on behalf of these bodies, act as direct purchaser or contractor vis-à-vis external contractors. In some cases, where the requirements are particularly specialised (e.g. Defence or Interior ministries), the CVI acts as a consultant, but the acquisition is directly managed by the ministry concerned.

According to the Ministry for Information Society, in 2001 mobile telephony had a 60% penetration of the market, ISDN had a 15% share and broadband transmissions were being introduced. The Government estimated Internet users to be around the 300-350 000 mark, with 20% of households having access to the Internet (110-140,000). An additional 10% of the households were considering an Internet connection by the end of the year. All households possessed at least one PC and felt that by 2002 they should have an Internet connection. SIOL, a spin-off of Slovenia Telekom is the main ISP, providing for 50% of all connections. The rest of the market is divided among another 39 national and international providers.

Practically all schools have had access to Internet since 1999 and 75% of the computers are connected. However, only 30% of pupils use the Internet for their education. There is 1 PC for 29 pupils in primary schools and 1 for 27 in secondary schools.

**Number of PCs In Slovenia**  
(Source: EITO Report 2001)



Regarding e-commerce, there is a gap between electronic banking transactions, which are common, and on-line sales, which are still limited to a small number of companies.

### ***Main ICT Regulatory and Legal Developments***

The government considers that only lower connection prices, more competition and more services will further the penetration of the Internet. In order to achieve these objectives, the following initiatives have been introduced. First, there is the HKOM (High-speed Communications) project, which has a number of essential goals. These are to increase the speed of all connections<sup>1</sup>; to unify call accesses, for ISDN and analogue connections; and to establish ATM (Asynchronous Transfer Mode) connections and test MPLS (Multi Protocol Label Switching). Further goals are to introduce a step-by-step changeover towards a unified protocol for the transmission of data (TCP/IP); to assure qualitative services through agreements regarding the assurance of the level of services (SLA); and to establish several separated virtual networks for the needs of individual groups of users (customs, taxes, courts, geodesic administration), allowing at the same time horizontal connections.

The most important issues considered by the governmental strategic document<sup>2</sup> are the integration of the various government departments through appropriate e-commerce practices based on the Dutch model.<sup>3</sup> A number of projects have been planned or launched to support the common functions of the Slovenian administration. There are ten main ones. Firstly, there is the automation of the administration, whose responsibility in the procedural field falls within the purview of the Interior Ministry. Secondly, there is the setting up of a decision-making support information system. Thirdly, there is an information system for the annual state budget drafting and supervision. Fourthly, a repository of laws and legal information,

---

<sup>1</sup> 128 Kbit/s for all users, 2MB/s digital connection between nodes and achieve 34 Mbit/s connectivity between the most loaded nodes

<sup>2</sup> The strategy of e-commerce in public administration of the Republic of Slovenia for the period from 2001 until 2004, drafted by the CIV, Ljubljana Sept. 2004

<sup>3</sup> Vertical relationships and connections are those between administration and citizens, economy and private sector. Horizontal one are those between different public departments, while the relationship with the Commission and the EU is considered a third special category.

including a site where the consultation of the official Slovenian law registry is open<sup>4</sup>. Fifthly, there is a human resources system. Another project is the establishment of a documentation centre regarding the accession of Slovenia to the EU. There is also a system for ICT public procurement and project management. An integrated electronic press review and paper clipping system, regarding national and some international press on the Slovenian government, has also been established. There is also the MVPDU-IT, a project management methodology in public administration for the field of information technology. Finally, there is EMRIS, a unified methodology for the planning and development of information systems.

The administration automation project includes the plan to digitise the personal records of public administration and one to create a database of all municipalities. Regarding personal records, the first step foresees the drafting of a new Personal Register Act. In a second phase, all administrative units across Slovenia will digitise current personal records and link them to the central registry of the Ministry of the Interior. Finally, other administrations such as maternity hospitals and hospitals will be included in the process.

The municipal database (known as Professional Support to Municipalities project) foresees the creation by the Ministry of Interior of a web page, including all essential data<sup>5</sup> and the registry of all municipal acts, also following current EU legislation. Among the projects already implemented, there is the electronic filing to request birth, marriage and death certificates, through a single portal ([e-uprava.gov.si](http://e-uprava.gov.si)) with a checking facility for the electronic signature of the applicant. Certificates are then delivered by mail. On 17 October 2001 the first four e-schools were opened, i.e. schools provided with free Internet access and the necessary technical assistance.

The main act regulating ICT business in the Republic of Slovenia is the Telecommunications Act. (*Zakon o telekomunikacijah*, in short *ZTel-1*), No. 326-08/94-3/26, adopted on 10 April 2001. It replaces a host of previous regulations such as five constitutional court rulings (years 1997, 1998, 1999, 2000) and the preceding Socialist Federation of Republics of Yugoslavia regulations on communications and post and (1978, 1988, 1989, 1990). The *Ztel-1* also includes more than 100 EU acts and recommendations that are part of the *acquis communautaire*. A further 20 regulations are in the process of being drafted and enacted in order.

Other important laws are the Immaterial Securities Act (passed by 23/3/1999) regulating the issue and transfer of electronic securities issued. It provides data protection for the holders of such securities and sets the management rules for the immaterial securities central registry. There is also the personal data protection act (8/7/1999); the ZEPEP or ECAS (Electronic Commerce and Electronic Signature Act), law 57/2000; and the UEPEP decree on the same matter (77/2000, 2/2001).

The main points of the *Ztel-1* include the institution of a regulating agency (Republic of Slovenia Telecommunications and Broadcasting Agency), whose functions are to notify the market as to which

---

<sup>4</sup> The site has been launched the 20/9/2001 (<http://zakonodaja.gov.si/>) and includes not only existing laws, but also projected amendments and local communities regulations. Parallel to the law repository runs a programme to support legislative procedure, enabling the administration to prepare bills and regulations with expert support.

<sup>5</sup> They include: contact data; administrative unit data (surface area, towns; central parts, size and structure of population, commercial activities); data on the mayor and the members of the municipal council and other related bodies; information about local education, employment structure, budget, closing accounts, major investments, types and volume of municipal funds.

public services are available; issuing specific licences to private operators (mobile public radio, fixed public telephony and broadcasting services); and monitoring the prices of major operators. This agency is independent, but its director is appointed by the government. Secondly, the National Assembly (i.e. the Parliament) nominates a consultative body of independent experts (the Telecommunications Council), whose function is to provide recommendations, to monitor the telecommunications market, to provide obligatory advice to the agency on certain issues and to monitor the agency's activity.

Other points include the adoption of the liberalisation principle, both for networks and services; the promotion of free access and competition to networks, with specific additional obligation for major operators; and the basing of prices on free market criteria, after a transition period which ends after April 2002. Subsidies are provided only to operators with less than 80% of the total national market share, provided they are present in public interest services such as fixed public telephone services (both domestic and international telephony).

Finally, under the Ztel-1, the main public operator, Telekom Slovenij, has to be privatised within the year 2002 and must provide such public interest services (in local legal parlance, universal services) without subsidy at least until 2003. The funding of such subsidies comes from licences fees. The government retains the choice to offer, via the operators, special assistance to users with special requirements and to expand the notion of universal services.

The Personal Data Protection Act specifies the criteria to be followed in order to protect personal databases. Government bodies, local communities and public officials are authorised to process only personal data as stipulated by the law. Those authorised by the law to collect personal data, can gather personal data relating to racial and other origin, political, religious and other beliefs, membership in a trade union or sexual orientation, only on the written approval of the individual involved, who must also be informed about how the data is used and for how long (art. 3). The confidentiality of this data must be particularly protected, including the use of encryption and appropriate electronic signatures.

The main aspects of the ZPEP law are that certification service providers do not need to obtain a special licence for their activity, but must notify the Ministry of the Economy in due time the commencement of their activity, the internal rules and procedures and means of signature creature and verification. The Ministry of Economy has the power to supervise the compliance of certification service providers with the stated rules and the legitimacy of their operations; inspections are carried out by designated officials who can by administrative decision confiscate data for 15 days, suspend or stop the operation of the service, revoke certificates which might be forged. The Agency for Telecommunications acts as an accreditation body for the voluntary accreditation of certification service providers.

### ***Assessment of Phenomena Undermining Dependability***

With the development of information and computer technology, new forms of crime were observed in Slovenia during the mid-90s. Cases of hacking have been known much earlier, but these were mainly acts of amateur hackers, with no or very limited damage to the targeted systems. Copyright abuse, especially concerning software, is a relatively widespread offence. Offences committed via the Internet are increasing and they include computer hacking; credit card fraud; illegal distribution of copyrighted material; juvenile pornography; theft of user names and passwords; and frauds committed against phone service providers.

The number of these types of criminal offences has been growing rapidly, although the reporting rate from citizens is still very low. The annual number of investigations opened on crimes involving ICT by

the police in this field by 2001 is approximately 500 (a fivefold increase compared with the last three years). Approximately 80% consist in the theft of telephone units, followed by forgeries using scanners (approx. 10%), whereas the most known cyber-crimes such as hacking and copyright infringement, account respectively for 6% and 4%.

Police statistics show that there were 21 computer crime cases investigated in 1995, 12 cases in 1996, 21 in 1997, 27 in 1998, 38 in 1999 and 38 cases in 2000 (the majority of them were computer piracy cases). The small numbers are mostly due to the fact that the statistics at the time only covered so called “pure” computer crime, where the computer was the “must” tool to commit the crime (no computer – no possibility to commit the crime). Other cases – so called “computer related”, in which a computer was used as an alternative tool to commit the crime (computer – the handy tool; commitment also possible without the use of the computer), were not included in the statistics, although there were incidents of such crimes.

By 2001, the police had introduced significant changes into the Crime Reporting System. It is now possible to monitor the data on all cyber-crime cases, whether they are pure computer crime or computer related crime. According to a new system, one counts all the cases and distributes them among specific articles of the Penal Code, whether the computer is used to commit the crime, or if the computer is the target of the criminal attack, or if the computer hardware/software is produced as a tool to commit the crime. The next table presents the situation of computer crime for the year 2001.

***Computer-Related Criminal Activities  
Reported by the Slovenian Police to the Judicial Authorities-2001***

<b>Criminal Activity</b>	<b>No.</b>
<i>misuse of personal data</i>	1
<i>violation of copyright</i>	1
<i>unauthorized exploitation of copyright work</i>	10
	13
<i>damaging of the computer data and programs</i>	1
	1
<i>breaking into the computer system</i>	6

*Source: Slovenia Ministry of Interior*

It is reasonable to suppose that with a better reporting rate and a greater security consciousness amongst all users, while keeping in mind the overall low crime rate in Slovenia, ICT investigations could double, whilst it is highly probable that the percentages of hacking and copyright violations could treble.

***Government Initiatives Aimed at Tackling Cyber-Security***

As mentioned, the legal text establishing the fundamentals of cyber-security is the Ztel-1 law. The issues of confidentiality and secrecy of transmitted data were key in the legislative debate on the monitoring of telecommunications, in accordance with the guidelines in the Criminal Procedure Act and the Personal Data Protection Act. Slovenian legislators ensured that relevant EC data protection legislation was incorporated (97/66/EC) in the national law.

The penalties foreseen for different types of disclosures and malpractice committed by the operators are in Ztel-1 financial. Legal persons risk a fine of 9,089-45,400 Euro (2-10 million Slovene tolar or Sit), if they do not appropriately protect the confidentiality of the information they are entrusted with as telecommunications operators or contained in the traffic of their customers. Additionally physical persons and security officers may incur in fines of 1,362-2,270 Euros (300-500.000 Sit), if they commit the same violations. Due to the process of harmonisation with the European *acquis*, the Penal Code may also include prison penalties for such infringements.

The ZEPEP law foresees penalties ranging from 2,270 Euro (500,000 Sit) to 22,700 Euro (5,000,000 Sit) for the most serious violations.

Relevant aspects of the UEPEP decree are requirements for physical and electronic protection and security controls throughout operation hours; double key requirement for the creation of signature data; separation between the management and issuing of qualified certificates, the management of the information system and that of protection and control; and the establishment within the CI of the SIGOV-CA (Slovenian Government Certification Agency) as the official public certification service provider for digital certificates.

Criminal law also includes different types of cyber-crime: theft and misuse of personal data acquired by penetrating a data bank; intrusion into a computer system; and the development of hacking tools. Moreover the Slovenian police has the investigative power to monitor and detect other types of offences, such as copyright infringement, forgery, pornography, and other computer-related crimes.

In order to counter cyber-crime, a special criminal police unit has been created. Moreover, the SI-CERT (Slovenian Computer Emergency Response Team) provides information and warning about concerning safety issues in Slovenian computer networks. It is also important to emphasise that the BSA has created a Slovenian branch office to foster the fight against copyright piracy.

The cyber-crime police specialists are part of the criminal police administration, but there is an increasing need to set up a specific cybercrime mission that would serve as a link between the specialists and the regular policemen. While there are still no legal and bureaucratic provisions for this mission, there is good co-operation with the judiciary (warrants for house searches and data acquisition from post offices and ISP). At a national level there is close co-operation between the Slovenian police, the BSA Slovenia, the SI-CERT and the Copyrights Agency of Slovenia. At international level there is a police partnership with the Italian police, which also facilitates international investigations.

At a preventive level, the Slovenian police use interviews and press conferences to inform the public, while SI-CERT and some Internet operators warn the users about the risks they might incur, complementing the activities of BSA Slovenia

In order to address operational shortcomings, the Slovenian police are following a phased strategy that encompasses both practical measures and legislative proposals. The first stage revolves around the acquisition and learning of advanced technical means and methods, whereas the second one advocates a simplification of the warrant issuing procedures, the possibility to conduct covert operations and the provision obliging the ISP to store data for a set time in order to allow pre-criminal investigations.

At the policy level, in the framework of the mentioned strategy of e-commerce drafted by the CVI, there is a strong realisation that significant progress has to be achieved regarding the dependability issues by 2004.

There are three main objectives to be reached. Firstly, there is the establishment of an adequate safeguard and protection policy (called project Safeguard and Protection Policy), using the experiences and solutions available and taking into account existing and future standards, with particular regard to the EU ones. This policy will encompass all types of risks - physical, accidental, technological, and all those due to criminal misuse. Secondly, there is the establishment of adequate supervision and control mechanisms, including a clear chain of responsibilities. Thirdly, there is an information effort towards public personnel and external contractors. In this regard, the strategy of e-commerce sets out the basic principles and means for the protection and confidentiality of data, as well as for general systems' reliability.

Part of the education effort will be done by the CIV in collaboration with the Administration Academy of the Ministry for Internal Affairs, involving the public administration personnel, on a large scale. On one hand, the focus will be on the change in administrative methods and organisation implied by ICT, but on the other, specific security training is plausible. At the moment the Academy is the leading educational institution in the field of public administration and has the required infrastructure (classrooms, equipment, professional and administrative personnel) for carrying out the expanded education programme.

Although Slovenia has adopted legislation in the field of the protection of personal data, which is in accordance with EU directives (95/46/EC), it is not always consistently observed when setting up information systems. The government foresees that in the future these rules will be increasingly stringent. The legislation itself is lagging behind new forms of crime and abuse such as, for instance, spamming, and there is still insufficient harmonisation between the level of criminalisation of certain offences in Slovenia and in other EU/OECD countries.

Additionally, the investigation of cyber-crimes is hampered by the fact that the ISP are not legally bound to store the data, which could help to identify offenders, and in any case this data must be acquired with a warrant. Investigation times become considerably longer when international co-operation procedures have to be followed.

Other loopholes derive both from insufficient international commitments and from specific gaps in the national legislation. As of February 2002, Slovenia was not yet able to sign the Council of Europe Cybercrime Convention. On the other hand, Slovenia is going through the procedure to sign the Cybercrime Convention and planning to complete it at the latest by May 2002.

At a national level the misuse of debit cards is not yet considered a criminal offence. In this case authorities have to resume the traditional charges of fraud or theft in order to prosecute the hacker. After the signature of the Cybercrime Convention, significant parts of the national telecommunications law as well as a number of procedures will be amended.

Some enhancement of security standards might be expected by two developments parallel in the civil arena. On 2 April 2001 Slovenia and the USA signed several agreements on scientific and technological co-operation, military training, security of classified military data, exchanges of technical information and co-operation on nuclear safety and in preventing the spread of weapons of mass destruction. With the probable inclusion of Slovenia among NATO members, the country's military will adopt stringent internationally agreed security and dependability standards, which the private sector may adopt.