# ORGANIZATION OF TECHNOLOGICAL STRUCTURES FOR PERSONAL DATA PROTECTION

*Irina Noninska, Radi Romansky**

Technical University of Sofia
Bulgaria

* Corresponding Author, e-mail: rrom@tu-sofia.bg

**Abstract:** Information security is an important part of the contemporary network world and is directly related to the protection of personal data. Various legal documents on the subject set out basic requirements for ensuring the privacy of users in the digital spice. The article presents a point of view for organization of an adequate data protection to implement the updated requirements of the latest regulation. A structure of a data protection system and organizational and technological means suitable for its implementation are proposed. Attention is paid to cryptographic protection and its application in personal data protection.

**Key words:** security, personal data, data protection, technological structures, cryptography.

## 1. INTRODUCTION

The formation of a clear concept of information security policy based on ever-changing information technology (IT) is an important prerequisite for successful personal data protection (PDP) [1, 2]. This defines the requirement of PDP policy to be considered as a component of the policy for information security (IT security policy) in all public, private and government organizations [3], including educational institutions [4].

The first standard for security policy (Trusted Computer System Evaluation Criteria – TCSEC, 1985, USA) defines it as a set of rules, standards, procedures and instructions for regulating the management, protection and dissemination of information. These basic components form the structural layers in a hierarchical organization, in which the IT security policy is responsible for ensuring the security of system and information resources in their physical organization and administrative management. This is very important in building and maintaining a reliable computer and network infrastructure that can successfully counter various attacks [5]. In this sequence, the PDP policy has the task of harmonizing the rules of IT security policy in order to define specific requirements for building the infrastructure for adequate and effective PDP. This is clearly stated in the General Data Protection Regulation (GDPR), in force since May 2018 [6].

Purpose of the article is to present a point of view for structural and technological organization of appropriate means to ensure reliable protection of the maintained registers of personal data in an organization. The construction of a protection system aims to counteract intentional or accidental attempts to influence information resources and to predispose them to unwanted violations and losses. In this respect, the next section presents the main structural components for adequate organization of PDP in an organizational unit. The third section is dedicated to technological and organizational measures for PDP, and the fourth section presents systems for cryptographic protection and its application in data protection cases. The conclusions presents some suggestions for correct work with personal data in the digital space.

## 2. MAIN COMPONENTS OF DATA PROTECTION

The main participants in the processing of available data are clearly defined by the regulations on the topic – data subject, data controller, data processor, data receiver and third party. Personal data (PD) provided with the consent of the owner (data subject) are organized in a register of personal data, which is the main structural unit with established rules for access and work with it. A clear requirement of the GDPR is that each organizational unit that is a data controller must establish and implement certain structures of organizational and technological measures to ensure a reliable PDP [7]. In short, this includes a system to regulate access to information resources, rules and instructions for legitimate handling of stored data and to determine an official to be responsible for PDP procedures.

➢ *System for PDP (SPDP)* is a set of interconnected technical, technological and organizational means to provide the necessary level of information security for automated and non-automated PD registers (Figure 1). It must have adequate means of information security and secure access to information resources, including the verification of access rights.

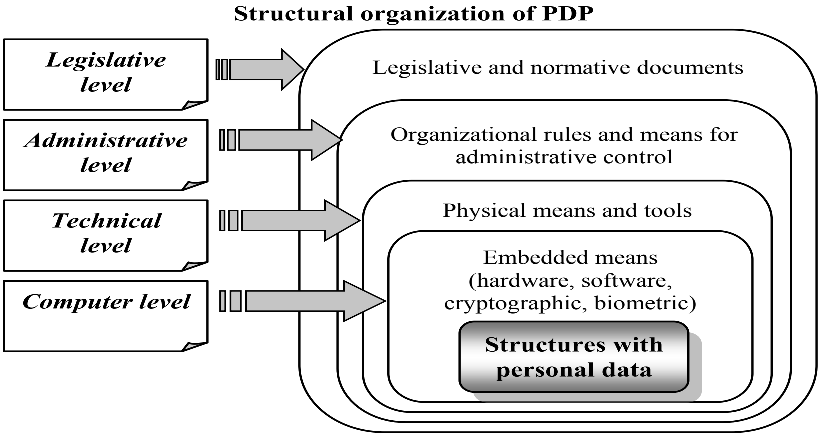
Structural organization of PDP
Legislative level
Administrative level
Technical level
Computer level
Legislative and normative documents
Organizational rules and means for administrative control
Physical means and tools
Embedded means (hardware, software, cryptographic, biometric)
Structures with personal data

*Figure 1. Structural organization of system for PDP*

The main requirements are for the SPDP to maintain authentication, authorization, accountability and integrity capabilities to counter attempts to compromise the security of information resources and in particular personal data profiles. These are the main elements of the CIA triad, applied in the evaluation of infrastructure solutions and software development. Indicative of the importance of the triad is the study presented in [8], which proposes to improve the voting system in the United States through the use of modern security technologies and cryptography.

➢ *Data Protection Guide (DPG)* – a set of rules for reliable information security, which are instructions for organizing and working with SPDP components at defined strict levels of access and priorities in PD processing, as well as their electronic transmission on communication buses . It should provide for measures to counteract force majeure (fire, flood, earthquake, etc., which occur infrequently but are unpredictable and cause serious damage) and technical errors that are more frequent, albeit more frequent but with but with less effect (errors of the operator or maintenance specialists, spread of virus programs, electromagnetic radiation, technical failures, etc.). A summary of the tasks assigned to DPG is presented in [9].

➢ *Data Protection Officer (DPO)* – an official authorized by the data controller with responsibilities and activities for the organization and management of technological structures and processes to ensure reliable protection of information resources. Performs the following main functions: defines the necessary levels of protection of different categories of data and determines the rules for access when working with personal data; is responsible for maintaining the SPDP and managing the creation and implementation of the DPG, as well as its updating if necessary; manages the restoration of information files in case of accidents and disasters or in case of breach of integrity as a result of illegal access; liaises with the state supervisory body.

## 3. TECHNOLOGICAL MEANS FOR DATA PROTECTION

Table 1 summarizes the required measures for ensuring a minimum level of adequate PDP from any form of illegal activity, especially in the case of electronic transmission.

*Table 1. Required measures for PDP*

| ***Technical & Technological measures*** | ***Organizational measures*** |
|---|---|
| ✓ Pseudonymization<br>✓ Encryption<br>✓ Confidentiality, integrity, availability and sustainability of processing systems<br>✓ Rules for the prompt recovery of "damaged" data when necessary and access to them<br>✓ Regular checks and evaluation of the effectiveness of the technical measures | ✓ Established internal rules for data protection<br>✓ Procedures regarding the provision of personal data to third parties<br>✓ Procedures for destruction of paper documents, archiving and destruction of copies on a digital medium<br>✓ Instructions on the organization, storage and use of personal data<br>✓ Regular evaluation of the efficiency of the organizational measures |

The basic structural levels of PDP organization are presented in Figure 1, as a proposal for the possible means for the implementation of the individual functionalities and requirements is presented below.

### 3.1. Embedded data protection tools at computer level

These are tools that are specifically designed for SPDP or use existing remedies. It is usually recommended to combine the capabilities of hardware, software, cryptographic and biometric tools. Their role in the PDP is significant because they are the last barrier to data against external attempts at unauthorized access. This requires them to ensure maximum security of the supported data.

▪ **Hardware tools for protection.** They are used to identify the legitimate user, to protect the processor, various devices in the system memory, to encrypt transmitted messages, etc. Depending on their functions, they are divided into the following groups:

➢ *Access control hardware* – used to identify the legitimate user or workstation, defining two main groups:

a) devices for identifying users by their individual characteristics (voice analysers, fingerprints, fingerprints or retinas, fingerprint and retinal analysers, signature comparison devices, etc.);

b) devices for control of access to certain places by checking a special secret code (from a keyboard, from a magnetic card, etc.).

➢ *External memory locking hardware* – provides protection against reading and writing parts of the disk or the entire disk, and different levels can be defined (individual sectors, individual files or groups of files, libraries, archives, etc.).

➢ *Hardware for control of local network communications with other networks*.

▪ **Software tools for protection.** They are used to recognize a password or PIN entered correctly by the user, to restrict access to parts of the disk, to check for virus software and to activate anti-virus programs, etc. The main groups are:

➢ *Software tools for user and workstation identification*: ✓ individual and group passwords with their periodic change; ✓ system for identification and authentication of users with maintenance of audit records; ✓ a question-and-answer check system.

➢ *Software tools for authorization* – defining and verifying access rights of individual users to specific data.

➢ *Software tools for control and signalling of violations*: ✓ in case of attempts for illegal access; ✓ maintaining a log file with information about the attempts made for unauthorized access; ✓ registration of virus programs and activation of anti-virus programs.

➢ *Special purpose software*: ✓ for protection of the OS and application programs; ✓ for servicing the data processing regimes for limited use; ✓ to define the level of secrecy of individual data groups.

▪ **Cryptographic tools for information security.** Cryptographic protection is an option for each source of a message to encrypt the text of this message (initial text) and to send the encrypted text (cryptogram) to another user in the system (Figure 2). The cryptogram is an incomprehensible sequence of characters obtained after encryption of the initial data. To read the cryptogram, it is necessary for the recipient to perform decryption by additional secret means. Both transformations (functions $f$ and $f^{-1}$) must be reversible and unique. Cryptology is a science with two parts: cryptography (data protection by encryption); cryptographic analysis (cipher detection).

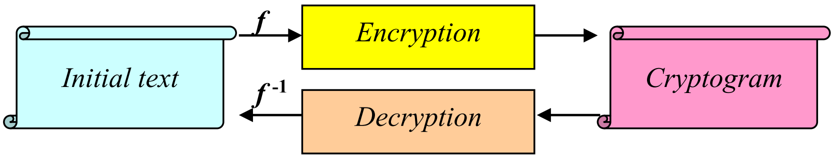

*Figure 2. Mine principle of cryptographic protection*

The means for cryptographic protection can be realized as a hardware or software systems (see the next section) by using symmetrical or asymmetrical algorithms. Systems with different purposes are used – for classification of the necessary data and messages, for authentication (authentication), electronic signature, etc.

### 3.2. Protection means from the external levels

■ **Physical means for protection at the technical level.** These are means that prevent access of outsiders to sites and halls related to information processing processes: ✓ locking of the premises with workstations, as well as the workstations themselves and the media (diskettes, CDs, etc.); ✓ distinctive signs or magnetic cards for users' access to the respective premises; ✓ providing security alarms and security; ✓ network segmentation and isolation of the database server from the Internet; ✓ separation of all servers in a special room and providing backup power for them.

■ **Organizational tools for administrative contro**l. They are used to expand the functions of physical means of protection, with special attention paid to the proper use of the provided hardware and software. This group includes: ✓ periodic inspection of users and tracking of their actions with the system; ✓ verification of compliance with the password change requirements; ✓ keeping backup of the most valuable data; ✓ defining levels of data security and access rights; ✓ determine the authority of the database administrator to control access to the relevant data; ✓ conducting various courses for further qualification of staff.

■ **Legislative and normative means for protection.** Based on special laws, documents and regulations introduced to ensure the security of computer systems and providing sanctions for violators. This is the last level of the protection scheme and in the technological point of view its role is relatively small.

## 4. TECHNOLOGY OF CRYPTOGRAPHIC PROTECTION

### 4.1. Cryptographic system

The cryptographic system is an implementation based on methods and means for encryption and decryption, in which the information is transformed in such a way that its content cannot be understood. Cryptographic systems are divided into two major groups, depending on the type of cryptographic key used and the specifics of the encryption and decryption procedures:

1. *Systems with a secret key* (Figure 3) – in which the encryption of the explicit text (P) to the cryptogram (C) is done with the secret key (SK), which is the same for both

users. Decryption of C to obtain the text P can only be performed if the same key SK is used.

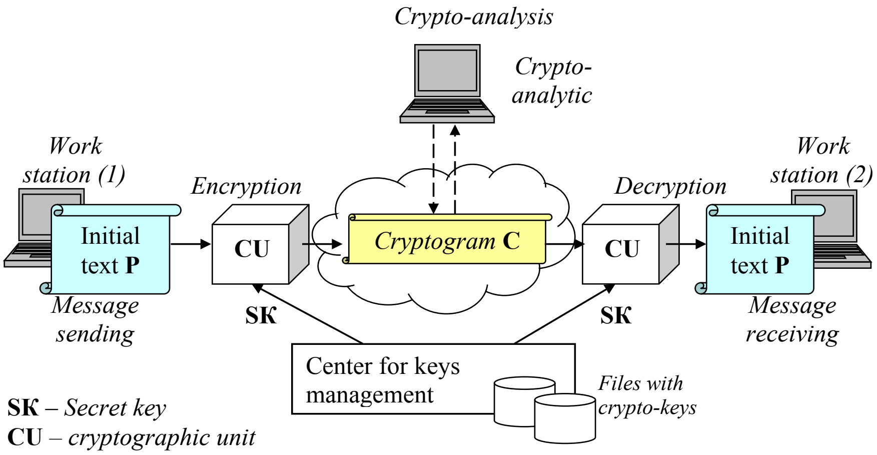

*Figure 3. Cryptographic system with secret key*

2. *System with a public key* (Figure 4) - they are characterized by the fact that for each user a key pair PK / SK (public / secret) is defined, as PK serves to encrypt the preliminary text and is publicly available to all users of the system, and SK is used only for decryption and is personalized for each individual user. In order to encrypt the text P from workstation (1) intended for workstation (2), the key PK2 must be used, which is accessible to both users (all public keys are publicly available). The cryptogram C is decrypted from workstation (2) using the secret key SK2, owned only by the user (2).

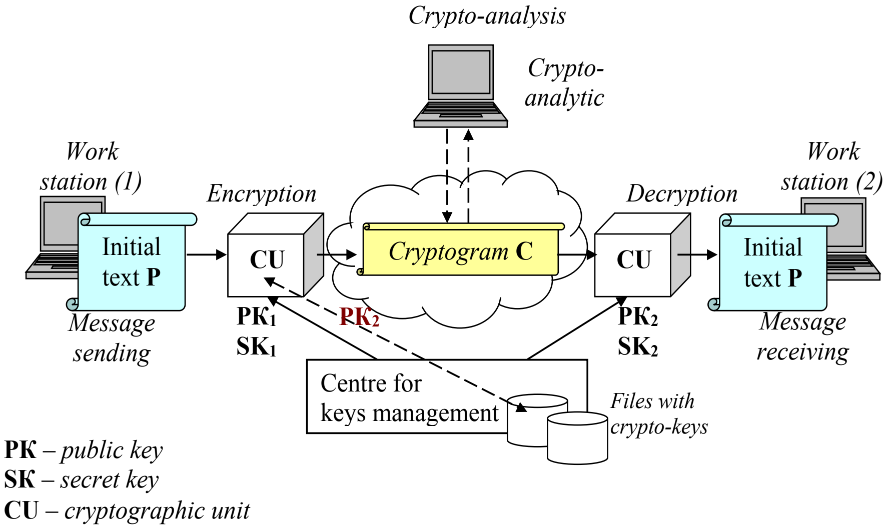

*Figure 4. Cryptographic system with a public key*

The cryptographic device CU from the schemes can be realized as a specialized hardware device, as a software system or through a combination of them.

The hardware type has a number of advantages, the most important of which are the following: ✓ higher speed characteristics compared to the software; ✓ protection from extraneous electromagnetic radiation and from direct physical impact; ✓ functionality and convenient operation.

Specialized software systems are characterized by flexibility and easy portability and are significantly cheaper than hardware devices, but have a lower processing speed.

In the combined implementation there is a certain division of the functions performed by the two parts according to their advantages and disadvantages. The main functions that are set in the hardware part are usually related to the generation and storage of keys – devices are used to protect against unauthorized access, as well as authentication of users using passwords stored on a smart card.

### 4.2. Protection when working in the network space

The contemporary digital age highlights the need for reliable protection of ever-increasing information resources in the network space. The importance of this task is also confirmed by the application of cloud services [10] and especially the growing intellectualization of activities through the development of Cyber Physical Systems (CPS) [11]. For example, in [10] an algorithmic approach is proposed for the application of the cloud in the network space for speech recognition in support of the activities of people with disabilities in smart home, traffic control in smart city and others. It is emphasized that cloud speech recognition services have advantages over classic stand-alone systems, such as "*the most important is a tight integration with the Internet and its users, which continuously feed the database and provide corrections*".

Effective protection of automated transport management systems in the contemporary smart society from various dangers and potential threats can also be ensured through the application of physical and cybersecurity [11]. The article emphasizes that key components of an intelligent transport traffic control system are at potential risk of being targeted by attackers who may use cyberspace as a conduit for malware. In this direction, a model study of the possibilities for strengthening the cybersecurity of critical infrastructure has been made.

All research in the network space, aimed at information security in the network space, discusses aspects of cryptographic protection, one of which is the protection of local workstations for access to allocated resources. The construction of an adequate protection system must support the following functions:

➢ Ensuring the confidentiality of data through encryption using high-performance encryption algorithms, embedding "transparent" for the user modules in the software, means for full or partial encryption of information on the hard disk, etc.

➢ Defining levels of data confidentiality and users' access rights to these levels.

➢ Authentication of users and prevention of illegitimate access to individual data by checking the user's PIN or other personal secret information from a smart card.

➢ Control over the means for encryption, identification and authentication and maintenance of a log file with data on the operation of the individual components for data protection, system and application software.

Due to the high probability of unauthorized access when transmitting data over a network, the cryptographic means used must meet the requirements summarized in Table 2.

*Table 2. Requirements for cryptographic tools when working in the network*

| ***Providing*** | ***Explanation*** |
|---|---|
| Confidentiality | Restricted access only of authorized users |
| Data integrity | Preservation of the structure and content of the data during storage and transmission through communication channels |
| Reliability | Defining the affiliation of the data to a specific source responsible for their veracity |
| Operability | Availability of the data necessary for a legitimate user at any time |
| Legal value | The information in the electronic document must be legally correct |

### 4.3. Encryption of archived data

The loss of personal data of customers or other persons with whom a company or organization works is a problem with significant direct (material) and indirect (moral) consequences:

✓ The direct costs are related to informing the clients about the loss, as well as the costs related to data recovery and overcoming the damages;

✓ Indirect costs are the consequences of damage to the brand, leading to a loss of credibility and a switch to another business company.

In order to avoid such problems, it is necessary to encrypt the archived data, because the archiving procedure provided by the respective database is not sufficient protection. Moreover, archived data carriers can change the place of their physical storage within the company. However, when deciding to encrypt archival data, possible risks must be analysed, for example:

✓ Failed encryption can be detected only the next time the archived data is accessed (which may not happen).

✓ Danger of losing the encryption keys, in which case the archived data will not be readable.

✓ Poor management of crypto-keys – unauthorized access to the key would make the encryption system useless.

✓ Changing the encryption keys will result in inability to access archived data encrypted with old keys.

There are three main ways to encrypt archived data.

➢ *Encryption at the source.* A software environment is used, which encrypts the data during its work and archives them in the encrypted form in which they are in the system. The disadvantages are the reduced performance of the file system (encrypting a file when writing and decrypting it at each reading), the use of the file system's own encryption keys (complicates the general management of keys), and inability to further compress the information during archiving data cannot be compressed). Therefore, this approach is recommended when processing small volumes of data.

- *Encryption by the backup software*. Encryption is done during the backup itself, and many backup software products offer similar options. The disadvantages are that these products in most cases have quite outdated key management systems, as well as reduced speed in the backup. This approach is also recommended for small volumes of data.

- *Hardware encryption*. A special hardware encryption device is used, through which the data passes when it is transferred to the media. The use of such a device allows to achieve high speed without delaying archiving, as the data is compressed before encryption. In addition, a more complex key management system is used, making it difficult for malicious access attempts. This approach is best suited for encrypting large amounts of data, but the disadvantage is that such devices are quite expensive.

## 5. CONCLUSION

The digital world allows access to and use of components such as websites, distributed resources, content, libraries, forums, social media, cloud services, etc. Most people use the Internet to expand their knowledge, social contacts and relationships, to exchange information and access various resources. This requires serious attention when using the opportunities offered by modern technologies and knowledge of the positive and negative ones of network communications and services. The latter requires a sufficiently good level of digital literacy regarding the digital age and personal data protection requirements [12].

## REFERENCES

[1] Romansky, R. Privacy and data protection in the contemporary digital age, *International Journal on Information Technologies and Security*, Vol. 13, No. 4, 2021, pp. 99-110.

[2] Romansky, R., I. Noninska. Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*. Vol. 17, No. 5, August 2020, pp.5288-5303 (article MBE2020268), DOI: 10.3934/mbe.2020286

[3] Romansky, R., I. Noninska. Business Virtual System in the Context of E-Governance: Investigation of Secure Access to Information Resources. *Journal of Public Affairs*, ISSN: 1472-3891, E-ISSN: 1479-1854, UK, John Wiley & Sons, Inc., Vol. 20, No 3, August 2020, e2072; (https://doi.org/10.1002/pa.2072)

[4] Zaslavskaya, O.Y., Zaslavskiy, A.A. Bolnokin, V.E., Kravets, O.Ya. Features of Ensuring Information Security when Using Cloud Technologies in Educational Institutions. *International Journal on Information Technologies and Security*, Vol. 10, No. 3, 2018, pp. 93-102.

[5] Zimba, A., Mulenga, A. A Dive into the Deep: Demystifying WannaCry Crypto Ransomware Network Attacks via Digital Forensics. *International Journal on Information Technologies and Security*, Vol. 10, No. 2, 2018, pp. 57-68.

[6] Tzolov, T. Data model in the context of the General Data Protection Regulation. *International Journal on Information Technologies and Security*. Vol. 9, No. 4, 2017, pp. 113-122.

[7] López, C. T., Domingo, I.A., Torrijos, J.V. Approaching the Data Protection Impact Assessment as a legal methodology to evaluate the degree of privacy by design achieved in technological proposals. A special reference to Identity Management systems. *ARES 2021: The 16th International Conference on Availability, Reliability and Security*, August 2021, Article 132, pp. 1-9. https://doi.org/10.1145/3465481.3469207

[8] Hoffman, L., Zahadat, N. Securing Democracy: A comparative look at modern and future US Voting systems through the lens of the CIA Triad. *Journal of Information Assurance and Security*. ISSN 1554-1010, Vol. 13, 2018, pp. 118-124.

[9] Dunham, B. ICO publishes revised data protection guide. *Journal of Direct, Data and Digital Marketing Practice*, Vol. 16, 2015, pp. 232–233. https://doi.org/10.1057/dddmp.2015.14

[10] Škraba, A., Stanovov, S., Semenkin, E., Koložvari, A. Davorin Kofjač. Development of Algorithm for Combination of Cloud Services for Speech Control of Cyber-Physical Systems. *International Journal on Information Technologies and Security*, Vol. 10, No. 1, 2018, pp. 73-82

[11] Ivanova, Y. Modelling the Impact of Cyber Threats on a Traffic Control Centre of Urban Auto Transport Systems. *International Journal on Information Technologies and Security*, Vol. 9, No. 2, 2017, pp. 83-95

[12] Romansky, R. Digital age and personal data protection. (ISBN: 978-620-4-73546-1), LAP LAMBERT Academic Publishing, 2022, 124 p.

### *Information about the authors:*

**Irina Noninska** is Associate professor in Cryptography and data security and PhD in Databases and Local Area Networks. Her scientific and research interests are in the area of Information and Network Security, Data Protection, Cryptographic Algorithms and Protocols, Quantum cryptography, Cyber security, Internet of Things, Telecommunication Standards. She is author and co-author of more than 90 scientific papers, articles and 11 books and chapters in books. She is a member of: Union of Scientists, Bulgaria; Union of Automatics and Informatics; International Editorial Board of International Journal on IT and Security; Organizing and Program Committee of Information Technologies.

**Radi Romansky** is a full professor at Technical University of Sofia, Doctor (Dr) in Computer Engineering and Doctor of Science (D.Sc.) in Informatics and Computer Science; Full member of European Network of Excellence on High Performance and Embedded Architectures and Compilation (HiPEAC). He has over 215 scientific publications and over 25 books. Areas of scientific interests: ICT, informatics, computer architectures, computer modelling, privacy and data protection, etc.

**Manuscript received on 10 January 2022**