NCS: Lab 1 - Security Compliance

Name: Mohamad Nour Shahin, Yehia Sobeh, Ali Hamdan, Matvey Makhnov

Group number: B22-CBS-01

Introduction

IT systems process/store/transmit sensitive and confidential data that can be certified by various standards - best practicies applied in the industry. But, it’s voluntary and depends on the organisation policies.

However, some data require mandatory compliance with the established requirements. Among such data there could be personal data and data constituting banking secrecy (card data, payment information, transactions, etc.)

Assignment

- For the assignment choose one of the data types that you will follow - banking data or personal data and analyze the local security regulation for this data type:
    - for personal data, analyze the GDPR and Federal Law 152-FZ.
    - for bank data - analyze PCI DSS and Bank of Russia Regulation No. 719-П
- To complete the assignment, prepare the summary report (2-3 pages long) where you could specify the following details:
    - Main purpose of a document
    - When it is mandatory to follow this regulation
    - Type of information this document is intended to (classification if applicable)
    - Summary of main points and requirements
    - Your contemplation and judgement (conclusion)
- Assignment can be done within a group of 3-4 people (mention names in the report). Make group in a way that english speaking students can work on the international regulation while russian speaking on the russian one accordingly.

Solution:

Analyzing of the General Data Protection Regulation (GDPR)

Main purpose of a document:

The purpose of the GDPR is to protect individuals inside EU or EEA and the data that describes them and to ensure the organizations that collect that data do so in a responsible manner

When it is mandatory to follow this regulation

The General Data Protection Regulation (GDPR) is mandatory when:

- The organization is based in the EU or EEA – Any organization operating within these regions must follow GDPR if it processes personal data from individuals there.
- The organization is outside the EU but serves people in the EU – If you provide goods or services to people in the EU, even for free, you're required to follow GDPR.
- When observe the actions of people in the EU – This includes tracking their behavior, profiling, or analyzing their data for insights.

Type of information this document is intended to (classification if applicable)

We have 3 types of it:

1. Personal Data: Information relating to an identified or identifiable person (name, ID number, location data, online identifier, etc.).

2.Special Categories of Data: Sensitive data needing higher protection (racial or ethnic origin, political opinions, health data, etc.).

3.Non-personal Data: Data that does not identify individuals, which may be subject to fewer restrictions (such as weather data, stock prices, data from anonymous IoT sensors).

Summary of main points and requirements

1. Lawful Data Processing: Organizations need a lawful basis to process personal data, like consent, contract performance, legal obligation, or legitimate interest.

2. Individual Rights: GDPR gives individuals rights over their data, including access, correction, deletion, and the right to object to data use.

3. Transparency and Purpose: Data collection must be transparent, and individuals need to know why their data is being collected.

4. Data Security: Organizations must take steps to protect personal data from unauthorized access or leaks.

5. Breach Notification: If a data breach occurs, organizations must inform authorities quickly and may need to notify affected individuals.

Your contemplation and judgement (conclusion)

GDPR represents a significant step in protecting personal data, especially in today's digital age. It emphasizes transparency, accountability, and respect for individual privacy.

GDPR applies to any orgnaization in the world that process data of EU residents. This approach ensures that EU citizens data is protected no matter where it's processed.

For organizations, GDPR brings responsibility and stricter standards, which may present operational challenges — such as obtaining lawful consent, enabling data access and deletion upon request. But following this standards can enhance not only data security, but improve transparency and of course build strong and trust-based relationships with their users.

Analyzing of the Federal Law 152-FZ (On Personal Data)

Main purpose of a document:

The main purpose of Federal Law 152-FZ is to protect personal information in Russia. It sets rules for how companies and organizations can collect, store, and use people's information, aiming to ensure privacy and security for individuals.

When it is mandatory to follow this regulation

- An organization works in Russia and collects or uses personal data about people in Russia.
- An organization is based outside Russia but processes information about Russian citizens (for example, by offering services or products in Russia).
- A company needs to share information outside of Russia; in this case, it must follow extra steps to make sure data is safe.

Type of information this document is intended to (classification if applicable)

We have 2 types of it:

1. Basic Personal Data: General information such as names, contact details, and identification numbers.

2. Special Types of Data: Sensitive data that includes things like race, nationality, religious beliefs, health information, or criminal history. This type of information needs extra care and usually requires consent from the person.

Summary of main points and requirements

1. Legal Basis for Data Use: Organizations must have a valid reason to use personal data, like consent from the person or a contract.

2. Transparency: Companies must explain to people why they are collecting data, how it will be used, and what rights the individual has.

3. Data Security: Companies must use strong measures to protect personal data from being accessed or lost without permission.

4. Rules for Sending Data Outside Russia: Organizations can only share data internationally if the receiving country has similar protections or if special measures are taken.

5. Storing Data in Russia: If a company collects data about Russian citizens, it must keep this data on servers located in Russia. Only after storing it in Russia can they consider transferring it abroad.

6. Rights of Individuals: People have the right to know what information a company has about them, to correct it, and even to request its deletion if needed.

7. Parental consent: If individual under the age of 18 cannot legally consent to any form of data processing, consent must be acquired from the legal guardian or parental authority.

Your contemplation and judgement (conclusion)

Federal Law 152-FZ provides strong protection for personal data in Russia. It applies to federal state government bodies, state government bodies of constituent entities of the Russian Federation and any organization that collect and process data for commercial purposes.

The rule about storing data in Russia makes sure the data of Russian citizens is kept within the country's control, which is an important focus for privacy and security.

For companies, following this law shows that they respect the privacy rights of individuals, and it helps build trust between companies and their users. While it can be challenging to keep data only in Russia, the law is clear about the steps companies must take to protect people's information.
