ASTANA IT UNIVERSITY

Report
Assignment 5

Student of group: CS-2115N
Full name: Adil Ergazin
Tutor: Zhanshuak
Zhaibergenova

Astana 2023

Assignment 5

Objectives

Part 1. GDPR compliance analysis

Part 2. GDPR compliance results

Part 1. GDPR compliance analysis

Chapter 4: Controller and processor (50%)

1. **General obligations (10%)**
    a. **Responsibility of the controller**

        By considering some factors such as the nature, scope, context, purposes of processing, and ranked risks for the rights and independence of individuals, the appropriate policies, standards, and technical measures realized by the controller were completely explored and viewed in the possession of regular updates. Furthermore, for data protection, the whole process of data protection possesses strong encryption and is linked to standards to be secured. Hence, by the PSI DSS certification, compliance with other protection systems, and data-guard aspects around restricting access and other actions contained in ISO 13335-3-2007 conclude the responsibilities of the controller.

    b. **Data protection by design and by default**

        By considering the design of data protection's factors, such as the art, cost, scope, context, purposes of processing, and ranked risks for the rights and independence of individuals, the appropriate policies, standards, and technical measures realized by the controller were completely explored and viewed in the possession of regular updates and by default data secure processes configured to acquire only necessary data as passwords and logins. Furthermore, for data protection, the whole process of data protection possesses strong encryption and is linked to standards to be secured and covered with monitoring. Hence, by the PSI DSS certification, compliance with other protection systems, and data-guard aspects around restricting access and other actions contained in ISO 13335-3-2007 conclude the responsibilities of the controller.

    c. **Joint controllers**

To control the processes and processors, only one controller is included in controlling processors.

d. Representatives of controllers or processors not established in the Union

The representative of the EU appointment was accorded to the controller, but basically two members of the project were represented: the administrator as the controller and the system administrator of the server as the processor. But the responsibilities of the controller are only two and are desired for monitoring and as a representative of the EU. Therefore, there are no complex confusions arising from the controller's engagements.

e. Processor

The processor role is dependent on our sys admin. But the processor's duties are controlled by the controller, exactly by our administrator (programmer). All duties related to processor processing are handled by one processor by contract and documents, and there is no sharing with others on account of possessing only two members in the project.

f. Processing under the authority of the controller or processor

By standards, two individuals, the controller and processor, did not possess the duties of processing the personal data, even under the authority of the controller, because they were encrypted and under security.

g. Records of processing activities

After each of the three audits, the records of processing activities done by Article 30 GDPR.

h. Cooperation with the supervisory authority

The controller and processor are cooperating with the supervisor; the controller's duties are also related to the supervisor's. The supervisor's duties rested on the controller, because the administrator (programmer) was tasked with managing and possessing the controller's duties.

2. Security of personal data (10%)

a. Security of processing

By considering factors, such as the art, cost, scope, context, purposes of processing, and ranked risks for the rights and independence of individuals, the security of processing is covered with ISO 13335-3-2007 with encryption system of data and the risk evaluation done by controller and processor were completely explored and written in the security policy of the project.

b. Notification of a personal data breach to the supervisory authority

The notification is periodically (by periodically monitroing) notified by the controller, who possesses the duty of the supervisor. Because the controller

administrator (not only the programmer but also the information security specialist).

c. **Communication of a personal data breach to the data subject**

In the event of a data breach, the controller would promptly deliver a communication to the data subject.

3. **Data protection impact assessment and prior consultation (10%)**
   a. **Data protection impact assessment**

   Data protection impact assessment relies on the necessity of a consultant, depending on the controller's duties as a programmer, administrator, and information security specialist, to consult on risk assessments.

   b. **Prior consultation**

   The prior consultation would rely on the 3 varieties of audits and interior audit of the controller as an information security specialist.

4. **Data protection officer (10%)**
   a. **Designation of the data protection officer**

   The designation of the data protection officer would be the controller, because his duties included those of an information security specialist in data protection and whole project also.

   b. **Position of the data protection officer**

   The controller on duty of the data protection officer possesses advanced knowledge in data security and must possess access to data without processing needs.

   c. **Tasks of the data protection officer**

   The tasks of the controller on duty and the data protection officer include monitoring the web application's processes and notifying them periodically.

5. **Codes of conduct and certification (10%)**
   a. **Codes of conduct**

   In the codes of conduct, all of the standards are regulated and correspond to our project's security policy.

   b. **Monitoring of approved codes of conduct**

   The monitoring of approved codes of conduct is regulated and corresponds with GDPR compliance and others, such as PSI-DSS and ISO.

   c. **Certification**

   The project relied on data protection certificates that included PSI-DSS compliance and were approved by the ISO 13335-3-2007 standard.

d. **Certification bodies**

The certification bodies were approved by one certificate of PSI-DSS compliance possessing encryption systems and also monitoring tasks for the data protection officer, which corresponded to the GOV ISO 13335-3-2007 standard. Furthermore, the security policy of the project would be periodically updated every 5 years updated.

Chapter 5: Transfers of personal data to third countries or international organisations (50%)

1. **General principle for transfers (7.14%)**

   All the statements corresponded to GDPR article 44.

2. **Transfers on the basis of an adequacy decision (7.14%)**

   All the statements corresponded to GDPR article 45.

3. **Transfers subject to appropriate safeguards (7.14%)**

   All the statements corresponded to GDPR article 46.

4. **Binding corporate rules (7.14%)**

   All the statements corresponded to GDPR article 47.

5. **Transfers or disclosures not authorised by Union law (7.14%)**

   All the statements corresponded to GDPR article 48.

6. **Derogations for specific situations (7.14%)**

   All the statements corresponded to GDPR article 49.

7. **International cooperation for the protection of personal data (7.16%)**

   All the statements corresponded to GDPR article 50.

Part 1. GDPR compliance results

Report

This assignment indicated the 27 articles by which the project's GDPR compliance must be greater than 80%, and on account of that, the 27 articles were split into 12 parts by generalizing them (5 segments of controller and processor, 7 segments of transfers of personal data to third countries or international organisations). Furthermore, the two chapters were divided 50/50 to reveal the percentage of each chapter. In order to be precise, in the second chapter, the project corresponded with GDPR compliance articles. And it is rated at 50% of the maximum. By navigating to the first 5 segments of the first chapter, they were forked at 10% for each segment. If we consider the security of personal data, which is

subdivided into 3 subsegments, two of them are rated at 3.3%, and the notifying part is rated at 3.4%. But because of rating their content, the last two of the three subsegments were evaluated at half of the rated score by dividing notification part 3.4 by half as 1.7%, the last one at 3.3% by half as 1.65%, and the beginning one at 3.3%. The security part was rated at 6.65% of the sum of the three subsegments. And according to the articles' full compliance, the other 4 parts ranked at 10% of the maximum.

In conclusion, by summarizing the whole two chapters and their segments, it is summarized at 50% of the second chapter, and the first one is at 46.65%, and in the final step, the satisfactory result is greater than 80%, revealing GDPR compliance at 96.65%.