



GDPR Compliance: Summary Post

Course: MSc Computer Science

Module: Network and Information Security Management

Assignment: ePortfolio

Date: Saturday 30th October 2021

Student ID: 126853

Post:

With the increase of IoT devices and Social Media networks, far more personal information is becoming available to Data Controllers. In 2018, the General Data Protection Regulations (EU) came into effect, bringing the rights of data subjects and responsibilities of data controllers into the modern age.


Organisations should ensure that they implement appropriate means to process data subjects information securely; encryption is one suitable method considered by the UK ICO (Information Commissioners Office, n.d.). A proper, non-vulnerable encryption method should be chosen to reduce the risk of information disclosure in the event of a breach. However, this does not reduce the organisation's responsibilities to ensure systems are appropriately secured.

Myself and all of my peers had researched a series of different case studies, all relating to breaches of the legislation and the action which the 'responsible authority' (Irish Data Commissioners Office) had taken against the organisations involved. In particular, my chosen case study was the illegal disclosure of CCTV footage of an individual to their employer, without adequate site notices or Privacy Notices being available. Unfortunately, the case study didn't highlight the action taken by the regulator, but presumably, there would be significant fines.

In most cases investigated by my peers, I noticed that the common factor affecting the businesses was the lack of complete policies, documentation and data access control policies. In some cases, these features would have prevented the data breach in the first place - whereas, in others, it would have reduced the overall impact of the breach occurring. Providing the data controllers implemented these

policies and functions, it is entirely plausible that the regulators would have been far more lenient with their overall judgement and enforcement actions.

Screenshot:


Kieron Holmes

Summary Post
2 secs ago

With the increase of IoT devices and Social Media networks, far more personal information is becoming available to Data Controllers. In 2018, the General Data Protection Regulations (EU) came into effect, bringing the rights of data subjects and responsibilities of data controllers into the modern age.

Organisations should ensure that they implement appropriate means to process data subjects information securely; encryption is one suitable method considered by the UK ICO (Information Commissioners Office, n.d.). A proper, non-vulnerable encryption method should be chosen to reduce the risk of information disclosure in the event of a breach. However, this does not reduce the organisation's responsibilities to ensure systems are appropriately secured.

Myself and all of my peers had researched a series of different case studies, all relating to breaches of the legislation and the action which the 'responsible authority' (Irish Data Commissioners Office) had taken against the organisations involved. In particular, my chosen case study was the illegal disclosure of CCTV footage of an individual to their employer, without adequate site notices or Privacy Notices being available. Unfortunately, the case study didn't highlight the action taken by the regulator, but presumably, there would be significant fines.

In most cases investigated by my peers, I noticed that the common factor affecting the businesses was the lack of complete policies, documentation and data access control policies. In some cases, these features would have prevented the data breach in the first place - whereas, in others, it would have reduced the overall impact of the breach occurring. Providing the data controllers implemented these policies and functions, it is entirely plausible that the regulators would have been far more lenient with their overall judgement and enforcement actions.

References:
Information Commissioners Office. (n.d.) Encryption | ICO. Available from: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/> [Accessed 30th October 2021].

Reply Edit Delete

References:

Information Commissioners Office. (n.d.) Encryption | ICO. Available from:
<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/encryption/> [Accessed 30th October 2021].