Collaborative Discussion 2→

Initial Post

The General Data Protection Regulation (GDPR) was introduced by the European Union (EU), as a way of providing 'the fundamental right to the protection of personal data' (European Commission 2016). Personal data is defined by the European Commission (2016) as 'any information relating to an identified or identifiable natural person'. For example, addresses, bank details, name identifiers, and etc. Processing data lawfully involves,

- Collecting data for the specified purpose.
- Data is relevant and limited to the necessary purpose.
- Adequate and kept up to date when necessary.
- Processed Securely

Data therefore needs to be managed throughout its life, which is why organisations use Data Lifecycle Management (DLM) to abide lawful data processing. As explained by Miller et al (2018) DLM involves looking after data from its creation period, to being processed, stored and secured, to how it's used, the sharing of the data, and archiving the data to either be reused or destroyed.

My current employment is with a passenger transport company who carry out work based on local government contracts. We therefore work with multiple councils across the UK, and the best practices and GDPR compliance is followed by the guidance they provide. Consequently, I'll be using 'Essex County Councils' Privacy and Data Protection policies as my example for 'IT Code of Conduct'.

Essex County Council (2023) state how they only provide the necessary information that is required to fulfil our job responsibilities in passenger transport. Aligning with GDPR best practice stated by the European Commission (2016). The personal data that is processed includes addresses, names and healthcare plans. When storing and sharing personal data within the organisation, we ensure encryption and pseudonymisation is used. Encryption is the procedure of turning original text/data into an alternative form known as ciphertext (Chen 2022), so that only users with the correct 'key' can transfer ciphertext back to original text. Pseudonymisation is an extra layer of protection along with encryption. Pseudonymisation is the process of switching data with an alias or pseudonym (European Commission 2019). For work, we replace the name of passengers with identification numbers as a way of achieving pseudonymisation. This is a way of masking personal identifiers in case of data getting into the wrong hands.

Overall, GDPR is important for protecting personal information from being handled carelessly. For big organisations, not complying with the EU regulations can mean big fines. In 2022, the firm Meta, owned by Instagram, received a €405 million fine for violating children's privacy, by sharing email addresses and phone numbers. However, there is still a long way to go to implementing GDPR into the thoughts of all businesses. Especially small and medium sized businesses (SME). Majority of fines are placed on large companies where the risk is higher, often overlooking SMEs. With SMEs also having a smaller human and financial resources to comply with regulations (Freitas & Mira da Silva 2018). At my current workplace, we're looking to automation to abide with regulations. Recently, we have implemented a blocked account process, so that if staff members haven't used the app server to access relevant data from the database, they are frozen out of their account. This monthly check, helps to avoid members of staff who have left the business, still having access to personal data.

References

Miller, K., Miller, M., Moran, M. and Dai, B. (2018). Data Management Life Cycle, Final report (No. PRC 17-84 F). Texas A&M Transportation Institute.

Freitas, M.D.C. and Mira da Silva, M. (2018). GDPR Compliance in SMEs: There is much to be done. Journal of Information Systems Engineering & Management, 3(4), p.30.

European Commission. (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504 [Accessed: 11 June 2023].

European Commission. (2019) Communication: Data protection rules as a trust-enabler in the EU and beyond – taking stock (COM/2019/374). Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2019%3A374%3AFIN [Accessed: 11 June 2023].

Chen, J. (2022) Wlhat Is Encryption? How It Works, Types, and Benefits. Available at: https://www.investopedia.com/terms/e/encryption.asp [Accessed: 14th June 2023]

Nial, M. (2023) The Biggest GDPR Fines of 2022. Available at: https://www.eqs.com/compliance-blog/biggest-gdpr-fines/ [Accessed: 14th June 2023]

Essex County Council (2023) Privacy and Data Protection. Available at: https://www.essex.gov.uk/about-essexgovuk/privacy-and-data-protection[Accessed: 14th June 2023].

Peer Responses and replies

Nima Osman - Sunday, 18 June 2023, 10:05 PM

Hey Chris,

Your post was a very good read, and I found a lot of the points you stated to be interesting. It was informative to know what the GDPR laws informed, and the summary provided was useful. GDPR also allows many countries to adopt comprehensive data protection rules, allowing for more opportunities for data flow between commercial operators and public figure authorities (Communication, 2019).

I liked how you linked the Data management lifecycle to these laws and explained how it played a part in abiding by the law (Miller, 2018).

Your organisation using pseudonymisation to ensure the masking of the individual is an essential practice to ensure data, if leaked, does not compromise the individual. What other ways does our organisation ensure the safety of someone's data?

You mentioned that the majority of fines are placed on large companies where the risk is higher, using Meta as an example. According to the GDPR, non-compliance results in fines of up to 4% of an organisation's global annual turnover or 20 million euros (whichever is higher). Although Freitas and Mira da Silva (2018) state that medium-sized businesses do not often have the resources to comply, shouldn't this law be enforced on all companies, including medium-sized businesses? Do you think that giving these smaller companies exemptions results not only in a loss of confidence and trust from the public but also in companies not feeling the need to comply strictly with the GDPR principles?

References:

Communication (2019) Communication from the Commission to the European Parliament and the Council, European Commission. Available at: https://commission.europa.eu/publications/communication-commission-european-parliament-and-council-0_en (Accessed: 17 June 2023).

Freitas, M.D.C. and Mira da Silva, M. (2018). GDPR Compliance in SMEs: There is much to be done. Journal of Information Systems Engineering & Management, 3(4), p.30.

Miller, K., Miller, M., Moran, M. and Dai, B. (2018). Data Management Life Cycle, Final report (No. PRC 17-84 F). Texas A&M Transportation Institute.

Regulation (EU) (2016) Regulation (EU) 2016/ 679 of the European Parliament and of the council ..., EUR-Lex: Access to European Law. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (Accessed: 17 June 2023).

In reply to Nima Osman

Peer Response

by Chris Final - Sunday, 25 June 2023, 8:42 PM

Thanks for the kind words Nima. The introduction of GDPR by the EU has made organisations accountable for the mishandling of personal data. Giving consumers extra protection when their personal information is shared.

Pseudonymisation is a good measure for any organisation. In my opinion, encryption is more important. That's why we use technology like a Virtual Private Network (VPN) when working remotely, to ensure internet traffic is encrypted and anomynised. Username and Password setups are used for Database access, and only relevant access is given. (e.g. only access to Essex region, and not the entire business).

Freitas and Mira da Silva (2018) mention that the larger supply of labour a large organisation has over SME's, makes it easier for them to comply with GDPR. It doesn't mean that SME's are exempt, or have a 'free ticket' for when it comes to abiding these lawful procedures. It does make it harder for SME's to monitor compliance. This is why it's important for senior managers to enforce a work culture that puts personal data at the forefront of employees thoughts. Focus on putting protecting the consumer, rather than the organisation avoiding fines.

Richard Charnock - Tuesday, 20 June 2023, 9:16 PM

Hi Chris.

The sections of your post around some of the steps Essex County Council put in place to secure personal data got me thinking about some of the challenges that come when trying to share data between organisations. In the public sector, data sharing between partner organisations should offer real benefits to the organisations to improve services provided. Research undertaken by the UK Parliament in 2022, outlines that these opportunities are not always realised with organisations quite often risk averse due to lack of understanding of the law or having a lack of faith in the mechanisms to share data. Avoiding risks of data breaches or law breaking is seen as more important than leveraging benefits from sharing data. Do you think the law is well understood in your organisation so that data sharing can be realised within the law and the process of pseudonymisation provides a method to share personal data with confidence?

References:

UK Parliament Post (2022), Sharing Public Sector Data, Available at: https://researchbriefings.files.parliament.uk/documents/POST-PN-0664/POST-PN-0664.pdf [Accessed: 19 June 2023]

In reply to Richard Charnock

Peer Response

by Chris Final - Sunday, 25 June 2023, 7:27 PM

Thanks for your comments Richard. Working with multiple councils across the UK is how our organisation works. I wouldn't say that avoiding data breaches, and law breaking, impacts the benefits of data sharing. We need the relevant data to fulfill the contract. What I would say is that the procedures to access the relevant personal data, differs between each council. Different procedures and understanding of GDPR does mean that the ease of business alters between councils. That's why it's argued that GDPR needs to have sector specific regulations. Abraha (2022) gives evidence of GDPR regulations causing 'fragmentation, legal uncertainty, and inconsistent implementation'. This is what's seen in my current employment, as the current GDPR regulation is a blanket measure for the entire economy, leading it to open interpretation and therefore altering implementation.

References

Abraha, H.H (2022) A pragmatic compromise? The role of Article 88 GDPR in upholding privacy in the workplace. International Data Privacy Law, 12(4), pp.276-296.

Chiazamoku Okegbe - Saturday, 24 June 2023, 8:44 AM

Hello Chris,

I enjoyed reading your post. And it is interesting to know your organisation uses encryption and pseudonymization to share and store personal data. Tankard (2016) mentioned that one of the importance of using encryption when sharing data is that it controls who is eligible to access the data and be sure they are who they say they are. I believe using encryption and pseudonymization goes a long way to protect personal data and the organisation’s confidential documents from any form of the breach or when they enter the wrong hands.

In your last paragraph, you mentioned, that your workplace plan to adopt a “block account process”, how does your company aim to achieve that, and will there be room for exceptions in case of unforeseen emergencies or staff who didn’t access the database because they were on leave? Secondly, how do you think the EU can make SMEs adhere to the GDPR regulations and take them more seriously?

References

Tankard, C. (2016) What the GDPR means for business. Network Security 2016(6): 5-8. Available from: https://www.sciencedirect.com/science/article/abs/pii/S1353485816300563 [Accessed 20 June 2023]

In reply to Chiazamoku Okegbe

Peer response

by Chris Final - Sunday, 25 June 2023, 6:53 PMThanks for your reply. Encryption is an important process, and its usually a process used by all organisations, even if employees are unaware it takes place. One of the most common methods of encryption is the use a VPN. I'll go into more detail on my summary post about this technology.

Managing access to the database is relatively easy, and reverting access to an employees account is a two minute exercise. It's not the case of colleagues losing all information when blocking an account.

Furthermore, the use of big fines will always be a deterrent to negligence of personal data, for whatever size of firm. However, senior management in SME's should have the responsibility of enforcing a work culture, that put clients personal data the forefront of employees thoughts. As I've mentioned to other peers on my course, GDPR shouldn't be seen as just a 'tick box' exercise. Taking GDPR into the account of ever business step, ensures a professional approach is taken.

Summary Post

To summarise, the implementation of GDPR by the EU has helped to protect consumers personal information. Organisations are handling personal data with the thoughts of protecting consumers at the forefront of their mind. As mentioned, the risk of big fines have acted as a deterrent to the mishandling of personal information, with the firm Meta being fined €405 million for violating children's privacy (Nial 2023).

I refer to how SME's may struggle with compliance, more than larger organisations which is the views of Freitas & Mira da Silva (2018). My peer Nima responded to my 'initial post' with regards to her views of SME's being compliant. SME's aren't exempt from fines, despite larger organisations being the 'bigger fish'. Larger firms have a bigger supply of labour than SME's, making it easier to monitor compliance. The solution to SME's is for senior managers to show colleagues the benefits of protecting personal data and putting their clients' thoughts first. This adoption will help with the adoption of DLM, when working with large datasets.

The benefits of GDPR to consumers is great, however, the blanket measure for all sectors does cause 'fragmentation, legal uncertainty, and inconsistent implementation' (Abraha 2022). My peer Richard, talked about data sharing among different organisations. Due to GDPR being open to different interpretation, the way data is shared between my workplace and different local councils, is never the same. The ease of doing business becomes impacted, as mentioned by Abraha (2022). The need for sector specific GDPR regulation, would help to avoid misinterpretation and create a more effective red tape for economic activity.

The method of using both encryption and pseudonymisation is the most effective way of complying with GDPR. Talking with my peer Chiazamoku, password protection of files and database access is the most commonly known method of encryption, as it's easy to create and maintain. But the topic has been heightened with recent life events, causing much of the economic work force to work from home. As a result, the use of Virtual Private Networks (VPN) increased. VPNs encrypt internet traffic and anonymise data when working remotely, helping organisations protect their client's personal data. Pseudonymisation is an extra layer of protection in case data gets in the wrong hands, acting as a way of masking the true identity of a person by assigning a number instead.

References

Abraha, H.H (2022) A pragmatic compromise? The role of Article 88 GDPR in upholding privacy in the workplace. International Data Privacy Law, 12(4), pp.276-296.

Nial, M. (2023) The Biggest GDPR Fines of 2022. Available at: https://www.eqs.com/compliance-blog/biggest-gdpr-fines/ [Accessed: 14th June 2023]