

DATA PROTECTION & PRIVACY SAFEGUARDS

Kumar Sindhurakshit

*ETHICS, REGULATION AND LAW IN ADVANCED DIGITAL
INFORMATION PROCESSING AND DECISION MAKING*

Degree Title



Table of Contents

<i>List of Abbreviations and Glossary</i>	<i>2</i>
<i>List of Figures</i>	<i>3</i>
<i>Acknowledgements</i>	<i>4</i>
<i>Executive Summery.....</i>	<i>5</i>
<i>Introduction.....</i>	<i>6</i>
<i>Methodology.....</i>	<i>6</i>
<i>Section A - Literature review</i>	<i>7</i>
Definitions	7
Data Protection.....	7
Personal Data.....	7
Data Processing.....	7
Data Controller.....	7
Data Processor	7
Data Subject.....	7
Data Privacy and Protection Brief History.....	8
UK GDPR Introduction.....	8
GDPR Applicability in Research	9
Applicability of Data Privacy Laws in Pandemic Scenario.....	10
Challenges With Data Anonymization	10
Impact on Web Privacy	11
Current Debates Around Data Protection and Privacy.....	11
Conclusion.....	11
<i>Section B - Marriott Data Breach</i>	<i>13</i>
Data Breach.....	13
Data Breach Tends.....	13
Marriott Data Breach	14
Critical Issues/ ICO Findings	14
<i>Section C- Recommendations</i>	<i>15</i>
<i>Appendices.....</i>	<i>16</i>
References	16
Bibliography.....	17

List of Abbreviations and Glossary

Abbreviations

ATT	App Tracking Transparency
COVID	Coronavirus
GPS	Google Privacy Sandbox
GDPR	General Data Protection Regulation
ITRC	Interstate Technology and Regulatory Council
ICO	Information Commissioner's Office
OPM	Office of Personnel Management
TPC	Third-Party Cookies
U. K.	United Kingdom
U.S.	United States

Glossary

e-commerce	e-commerce (electronic commerce) is the buying and selling of goods and services, or the transmitting of funds or data, over an electronic network, primarily the internet.
e-governance	e-governance is about the use of information technology to raise the quality of the services governments deliver to citizens and businesses.
Equifax	An American multinational consumer credit reporting agency headquartered in Atlanta, Georgia and is one of the three largest consumer credit reporting agencies, along with Experian and TransUnion.
Equifax Data Breach	The Equifax data breach occurred between May and July 2017 at the American credit bureau Equifax. Private records of 147.9 million Americans along with 15.2 million British citizens and about 19,000 Canadian citizens were compromised in the breach, making it one of the largest cybercrimes related to identity theft.
Q-Legal	Q-Legal is a Queen Mary University London award winning service providing free legal advice and resources to start-ups and entrepreneurs.



List of Figures

Figure 1: Methodology used for literature review	6
Figure 2: History of data privacy laws and regulations	8
Figure 3: United Kingdom GDPR principles.....	9
Figure 4: Data breach trends	13
Figure 5: ICO findings in Marriott data breach case	14



Acknowledgements

Author would like to thank Queen Mary Q-Legal team members Amina Kabiru, Anjali Karunakaran and Rajat Datta for their support with presentation on laws governing data protection and Ms. Mahesha Samaratunga for her continuous guidance and support.

Author would also like to acknowledge the stakeholders who participated in the seminars and discussions and his colleagues and team members from previous jobs who gave up their time to share their experiences on data protection in general and GDPR particularly in telecom sector. Without these contributions, this work would not have been possible.



Executive Summery

Current digital age is witnessing an exponential proliferation of sophisticated hardware- and software-based intelligent solutions that are able to interact with the users at almost every sensitive aspect of our lives, collecting and analysing a range of data about us. These data, or the derived information out of it, are often too personal to fall into unwanted hands, and thus users are almost always wary of the privacy of such private data that are being continuously collected through these digital mediums. To further complicate the issue, the infringement cases of such databanks are on a sharp rise. Several frameworks have been devised in various parts of the globe to safeguard the issue of data privacy; in parallel, constant research is also being conducted on closing the loopholes within these frameworks. This study aimed to analyse the UK GDPR framework (Legislation.gov.uk, 2018) and other frameworks with focus on data protection and privacy by design identify the key challenges and proposed solutions. This research is based on a systematic literature review specifically in telecom , heath care, financial domains.

Introduction

Collection and processing of customer data has been crucial for providing digital services today be it telecommunication, health care, banking, tourism, e-commerce, e-governance or any other sector business cannot operate without collecting data at the same time there has been several incidences in the recent past where huge number of individuals personal data has been compromised so it is essential to have established process and regulatory framework to ensure safe processing of private data and protecting individuals from such breaches at the same time allowing business to collect and process data to offer various products and services to their customers.

In this paper we will introduce various terms associated with data privacy and review literature on data privacy regulations, frameworks, trends and challenges with conclusion on our findings.

Methodology

In literature review, lacking rigor is often considered as one of the most crucial or even critical factor, a lack of rigor in documenting the literature search process often causes problems regarding the reliability of a literature review (Brocke et al., 2009), to avoid this fundamental mistake, A systematic approach with the five steps of the workflow shown in figure 1 below to ensure a reproducible selection of the literature used to compile this review.

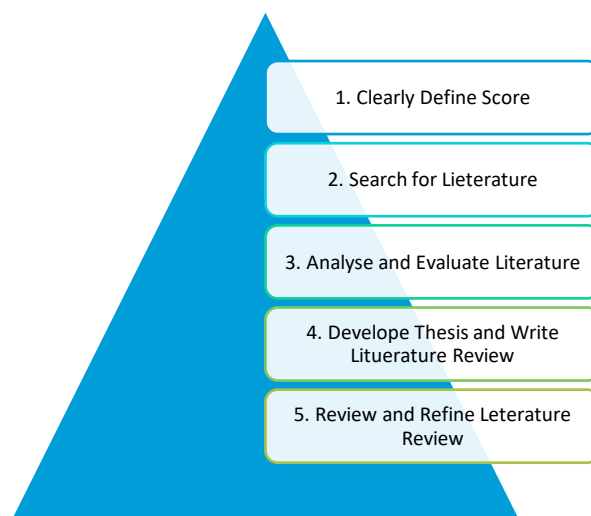


Figure 1: Methodology used for literature review



Section A - Literature review

Definitions

For consistency definitions presented here are taken from Information Commissioner's Office ICO (ico.org.uk, 2021), the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Data Protection

Data protection is the fair and proper use of information about people. It's part of the fundamental right to privacy – but on a more practical level, it's really about building trust between people and organisations. It's about treating people fairly and openly, recognising their right to have control over their own identity and their interactions with others, and striking a balance with the wider interests of society.

Data protection is essential to innovation. Good practice in data protection is vital to ensure public trust in, engagement with and support for innovative uses of data in both the public and private sectors.

Personal Data

Personal data means information about a particular living individual. This might be anyone, including a customer, client, employee, partner, member, supporter, business contact, public official or member of the public. It doesn't need to be 'private' information – even information which is public knowledge or is about someone's professional life can be personal data.

It doesn't cover truly anonymous information – but if you could still identify someone from the details, or by combining it with other information, it will still count as personal data.

Data Processing

Almost anything done with data counts as processing; including collecting, recording, storing, using, analysing, combining, disclosing or deleting it.

Data Controller

A controller is the person that decides how and why to collect and use the data. This will usually be an organisation, but can be an individual (eg a sole trader). If you are an employee acting on behalf of your employer, the employer would be the controller. The controller must make sure that the processing of that data complies with data protection law.

Data Processor

A processor is a separate person or organisation (not an employee) who processes data on behalf of the controller and in accordance with their instructions. Processors have some direct legal obligations, but these are more limited than the controller's obligations.

Data Subject

This is the technical term for the individual whom particular personal data is about, in this paper Data subjects are also referred as individuals , person or customer.

Data Privacy and Protection Brief History

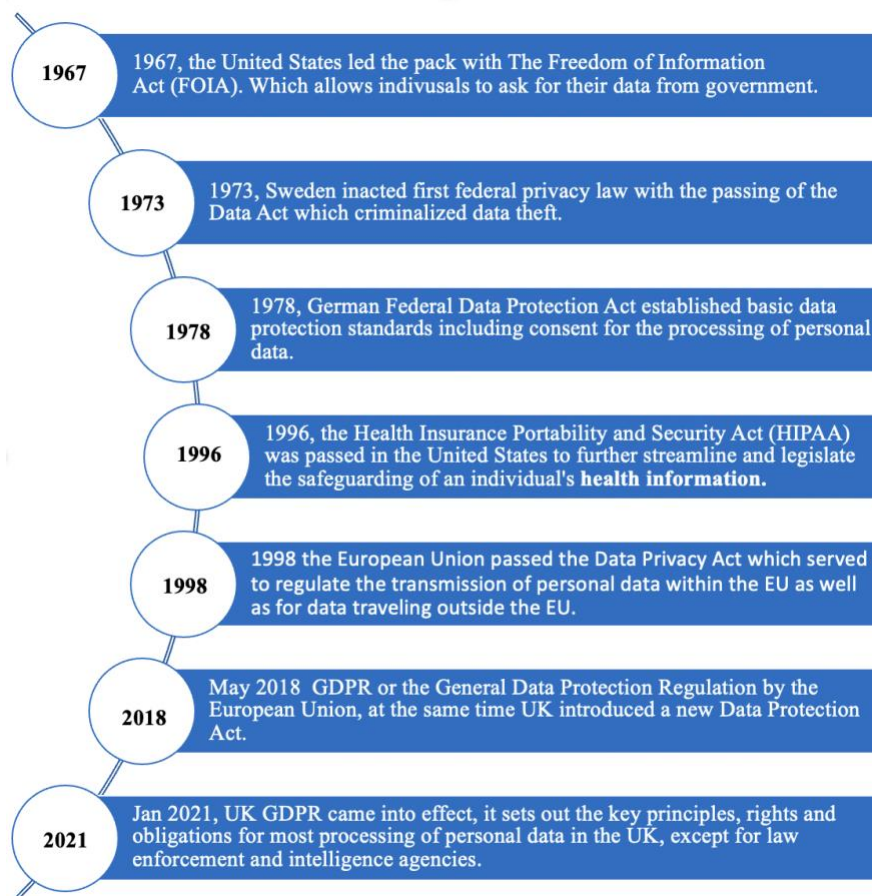


Figure 2: History of data privacy laws and regulations¹

UK GDPR Introduction

UK GDPR can be considered as the world's strongest set of data protection rules, which enhance how people can access information about them and places limits on what organisations can do with personal data. The full text of UK GDPR is collection of huge set of individual articles, provisions and is not in the scope of this paper.

At the heart of GDPR is personal data. Broadly this is information that allows a living person to be directly, or indirectly, identified from data that's available. This can be something obvious, such as a person's name, location data, or a clear online username, or it can be something that may be less instantly apparent: IP addresses and cookie identifiers can be considered as personal data.

Under GDPR there are also a few special categories of sensitive personal data that are given greater protections. This personal data includes information about racial or ethnic origin, political opinions, religious beliefs, membership of trade unions, genetic and biometric data, health information and data around a person's sex life or orientation.

The crucial thing about what constitutes personal data is that it allows a person to be identified – pseudonymised data can still fall under the definition of personal data. Personal data is so important under GDPR because individuals, organisations, and companies that are either 'controllers' or 'processors' of it are covered by the law. The strength of GDPR has seen it lauded as a progressive approach to how people's personal data should be handled.

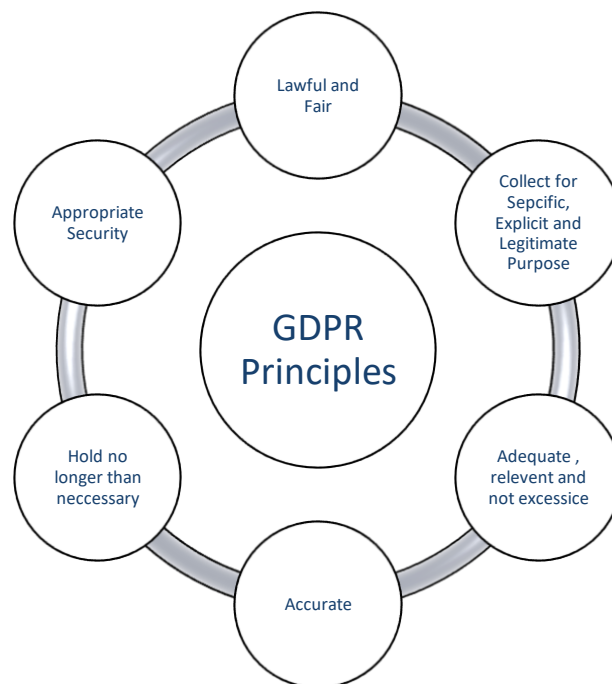



Figure 3: United Kingdom GDPR principles

GDPR Applicability in Research

Since innovation is crucial the exemptions for scientific research in the General Data Protection Regulation (GDPR) permit the reuse of personal data for research purposes. The GDPR defines scientific research in a broad manner, including publicly and privately funded research. This broad exemption aims to provide flexibility to conduct a wide range of scientific research. However, this definition permits private companies to conduct commercial research, and they might not have in place the same level of ethical and institutional safeguards as academic researchers. Furthermore, public interest does not have to be apparent in commercial research. Therefore, commercial AI research should not fit into the GDPR research exemption without public interest and similar safeguards as academic research.

The prohibition on solely automated decision-making in the GDPR may pose a significant hurdle for the application of AI in various fields (Meszaros and Ho, 2021). However, scientific research might be less affected, since mostly the main goal of research activities is producing new knowledge, rather than making decisions for individuals. It is crucial to differentiate between profiling and solely automated decision-making, since profiling without solely automated decision-making is not prohibited by the GDPR. The GDPR defines profiling as the automated processing of personal data to analyse or make predictions about individuals. For instance, predicting performance at work or personal preferences. Profiling is composed of two



main elements first the automated processing, which does not have to be solely automated, and second the purpose is to evaluate personal aspects about an individual. Profiling can be one of the sources for automated decision-making. In the case of speeding tickets, when the police automatically fine drivers based on data collected from a traffic camera system, it is automated decision-making based on observed data. However, when citizens' driving habits are evaluated to calculate their fines, such as previous offences, then the automated-decision is based on profiling.

Applicability of Data Privacy Laws in Pandemic Scenario

Regulatory frameworks like GDPR and UK GDPR providing the necessary legal architecture by which the handling and processing of the personal data can be managed, particularly in the context of health mobile applications, in order to be lawful, fair, and reflecting the underpinning social and ethical values (Christofidou, Lea and Coorevits, 2021). This brings an argument on the table as to the extent the data privacy laws UK GDPR had to and can be applied when this data and information are needed for research under time pressure, with a vital source of information being the amount of digital health data that can be collected. However, this way in turn gives rise to questions surrounding the ethics of using citizens' data in a seemingly broad manner and places the public interest and the privacy of individuals on opposite ends of the scale. Consequently, this way also leaves room to question whether it is time to re-evaluate data protection overall when it comes to the privacy of citizens in the time of pandemic.

In literature fears have been expressed over a "surveillance state", which may be justified given that the data gathered by the contact tracing applications are 'the most personal and intimate data a government has ever sought to gather about its own citizens' (Fahey and Hino, 2020), it is important to consider that perhaps in reality these fears may have little foundation. The use of contact tracing applications as indicated in literature and the mass media is conducted on a voluntary basis in Europe, a different approach taken than non-EEA countries such as China, India and Qatar all of which have legally mandated the use of the applications (Lucivero et al., 2020)

Challenges With Data Anonymization

Anonymizing datasets (ICO, Introduction to anonymisation Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance, 2021) through de-identification and sampling before sharing them has been the main tool used to address concerns on data privacy , however generative copula-based method (Rocher, Hendrickx and de Montjoye, 2019) was able to reidentify 99.98% individuals using 15 demographic attributes, similarly researchers at University of Texas demonstrates that an adversary who knows only a little bit about an individual subscriber can easily identify this subscriber's record in the dataset. Using the Internet Movie Database as the source of background knowledge, they successfully identified the Netflix records of known users, uncovering their apparent political preferences and other potentially sensitive information (Narayanan and Shmatikov, 2008)

These examples suggests that even heavily sampled anonymized datasets are unlikely to satisfy the modern standards for anonymization set forth by GDPR and seriously challenge the technical and legal adequacy of the de-identification release-and-forget model.



Impact on Web Privacy

The core web security mechanisms such as the same-origin policy pose problems for the implementation of consent according to GDPR rules, and opting out of third-party cookies requires the third party to cooperate. Overall, the web have become more transparent at the time GDPR and UK GDPR came into force, but there is still a lack of both functional and usable mechanisms for users to consent to or deny processing of their personal data on the Internet (Degeling et al., 2019). Author after interviewing a number of individuals have also found that the cookies and described usage is too complicated for the users and they end up accepting all in fear that website may not function properly if they do not accept all cookies compromising their privacy.

Current Debates Around Data Protection and Privacy

One of the key debates on data privacy are usage of “third party cookies” (TPCs) to track user activities on the browser to show relevant advertisements for the user. These technologies used in online advertising, and the way they are deployed, have the potential to be highly privacy intrusive. While the advertisers and proponents of such tracking argue that this tracking is indeed for user benefits as they get to see meaningful advertisement instead of seeing unrelated content the opponents argue that they are serious intrusion on individual privacy.

Understanding its criticality and impact on society information commissioner is working with key stakeholders to identify and implement alternative solution to remove the use of technologies that lead to intrusive and unaccountable processing of personal data and device information, which increases the risks of harm to individuals. This will ensure fair treatment of advertising industry, corporations and users. (Information Commissioner’s Opinion: Data protection and privacy expectations for online advertising proposals, 2021).


One of the most significant is the proposal by Google known as the “Google Privacy Sandbox” (GPS) (Google, 2022). The GPS intends to replace the use of third-party cookies (TPCs) and other forms of cross-site tracking with alternative technologies for enabling targeted advertising (and the measurement of advertising . Another prominent development is Apple’s “App Tracking Transparency” (ATT), which has had a notable impact – both in terms of the number of users exercising control over tracking, as well as the market itself .

Conclusion

The reviewed publications discuss how GDPR and similar stringent frameworks are supporting data privacy of individuals to a great extent , however there is also concern raised in literature particularly as there are no agreed and accepted framework across all nations , the protection and privacy of individual is highly dependent on the geography he or she is living.

There are also concerns on effectiveness of such frameworks in pandemic like situation where time of data sharing is so critically that it may lead to compromise of data or if firewalls are followed stringently then it may lead to delay in designing and implementing solution like contact tracking and covid research in general, which leads to compromise between individual rights and social good.

The author after analysing currents status of data protections and privacy, it pros and cons is of the view that that there is significant progress in data protection and privacy of individuals in past few years however yet there are major challenges like intrusive tracking with third party cookies which need to be addressed and improved. It is encouraging that organisations



like UK information commissioner are continuously engaged with key stakeholders to incessantly enhance the aspect of individuals data privacy without compromising innovation, benefits for business, users and society the data sharing brings. Author also discern that different data privacy acts are limited to specific geographies, countries leaving individuals in other geographies privacy is not protected. Different laws and interpretation of privacy also make it challenging for service providers, online advertisers to implement different policies based on the region creating implementation nightmare and error-prone, there is vital need of having uniform data privacy framework and protection in universal umbrella body like UN to ensure that it does not remain a geographically limited to certain countries and people living there to implement those state of the art data privacy mechanisms “Data Privacy Need to be Seen as Human Right”.

On the technology front author would emphasise that ensuring data privacy is not just one time act, it requires continuous review and research to ensure that an understanding and evolution of the state of the art in data protection and its implementation as technologies as society digital behaviour patterns evolves. There is also clear need to have pre-agreed protocols and data sharing mechanisms to be applied in pandemic like situations ex. COVID to avoid delays and faulty implementations.

Section B - Marriott Data Breach

Data Breach

A data breach means a rupture of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals (ICO, 2019).

Key motive behind data breaches are criminals stealing business' financial details, customer's financial details, sensitive personal data, customer's or staff email addresses and login credentials, customer databases, clients lists, making a social or political point through hacktivism, espionage or intellectual challenge also called as 'white hat' hacking and are normally carried out through weak and stolen credentials, back doors application vulnerabilities, malware, social engineering, physical attacks and human errors like unintentional disclosure or wrong configuration.

Data Breach Trends

As per ITRC 2021 annual report the overall number of data compromises (1,862) was up 68 percent over 2020, with the new record number of data compromises is 23 percent over the previous all-time high (1,506). To make matter worst only less than 5 percent take the most effective protective action after receiving a data breach notice (ITRC, 2022). The below picture describes key trends in the data breach -

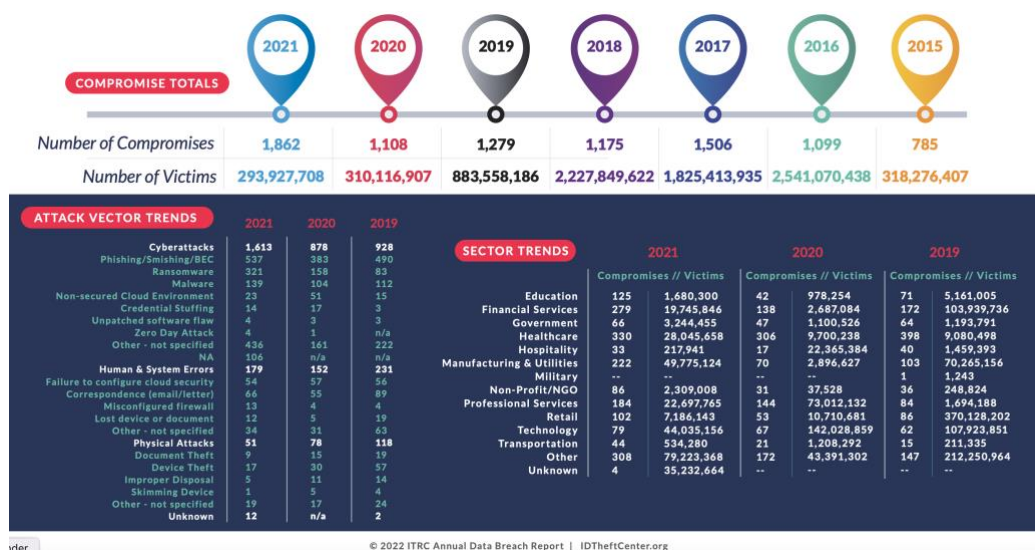


Figure 4: Data breach trends

Marriott Data Breach

In late 2018, the Marriott hotel chain announced that one of its reservation systems had been compromised, with hundreds of millions of customer records, including credit card and passport numbers, being exfiltrated by the attackers. While Marriott has not disclosed the full timeline or technical details of the assault, the ICO has fined Marriott International Inc £18.4million for failing to keep millions of customers' personal data secure.

The penalty was issued under the Data Protection Act 2018 for infringements of the GDPR. The GDPR sets out six basic principles organisations must comply with in processing personal data. These are: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; security; accountability. This penalty deals with failures by Marriott regarding the security principle.

One of the interesting fact (Farlinger, 2020) about Marriot data breach is the code and attack patterns used match up with techniques employed by state-sponsored Chinese hackers; the attackers used a cloud-hosting space frequently used by Chinese hackers, that none of those millions of valuable records have ended up for sale on the dark web; this wasn't a mere plundering raid. What would the motivation for the attack be, then? The government sources speculate that it was part of a broader Chinese effort to acquire massive amounts of data on American government employees and intelligence officers; Marriott is the top hotel provider for the U.S. government and military. The stolen passport numbers in particular could be used to track movements around the world.

In February of 2020, the United States Department of Justice formally charged four members of the Chinese military with the 2017 attack on Equifax that netted personally identifying information on millions of people; in the announcement of the indictment, the Equifax attack was explicitly linked to the Marriott and OPM breaches as part of the same larger operation. This was an extremely rare move — the U.S. rarely files criminal charges against foreign intelligence officers.

Critical Issues/ ICO Findings

The two key ICO findings were that the 72-hour breach notification rules had been infringed (GDPR Article 33 and breach of transparency and accountability

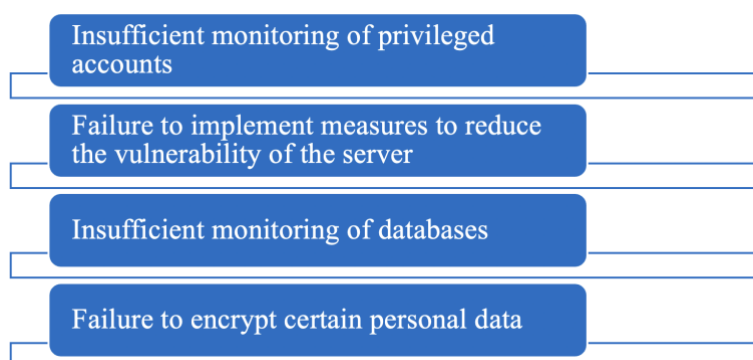


Figure 5: ICO findings in Marriott data breach case



Section C- Recommendations

ITRC report have some disturbing findings such as breach notice transparency is decreasing , notice effectiveness is low, and only less then 5% corporation take effective measures even after notice of breach (ITRC, 2022). Similar finding are also reported in other reports, these finding highlight the need of regulatory enforcement agencies like Information Commissioner and their role of defining regulatory framework and ensuring corporations take data privacy and data breaches more seriously with complaint procedures and autonomous actions on the data breaches.

Based on study and understand of current status and challenges author have below recommendations -

- Key learnings from Marriott case, are encryption keys need to be kept separately than encrypted data, proactive monitoring and actions as important as preventive mechanisms and mergers and acquisitions require critical scrutiny of data breaches and cybersecurity threats.
- Currently there is lack of standardised reporting of data breach , standardization of reporting need to be done on urgent basis to ensure everyone have same interpretation of reports.
- Regulatory agencies such as GDPR, ICO are imposing stricter rules, e.g., they are demanding disclosure of data breaches, imposing bigger penalties for violating privacy laws, as well as using regulations to promote public policies to protect information and consumers however there are no uniform standards to determine controls and procedures globally. There is strong need to have a global uniform regulations and control measures as cybercriminals are operating at global scale.
- Looking at various literature it is evident that currently there is lack of information exchange and collaboration between various stakeholders like different countries, governments agencies and other stakeholders , author recommends an international organization of trusted computer response teams dedicated to the prevention of data breaches and cyber security attacks.
- At the technology front there is need to develop intelligent platform which can anticipate, mitigate, and respond to data breaches and cyberthreats

Appendices

References

1. Brocke, J., Simons, A., Niehaves, B., Niehaves, B., Reimer, K., Plattfaut, R. and Cleven, A. (2009). RECONSTRUCTING THE GIANT: ON THE IMPORTANCE OF RIGOUR IN DOCUMENTING THE LITERATURE SEARCH PROCESS. ECIS 2009 Proceedings. [online] Available at: <https://aisel.aisnet.org/ecis2009/161/>.
2. Christofidou, M., Lea, N. and Coorevits, P. (2021). A Literature Review on the GDPR, COVID-19 and the Ethical Considerations of Data Protection During a Time of Crisis. Yearbook of Medical Informatics, 30(01), pp.226–232.
3. Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F. and Holz, T. (2019). [online] Available at: <https://arxiv.org/pdf/1808.05096.pdf>
4. Fahey, R. and Hino, A. (2020). COVID-19, digital privacy, and the social limits on data-focused public health responses. International Journal of Information Management, [online] 55, p.102181. Available at: <https://www.sciencedirect.com/science/article/pii/S0268401220310239>.
5. Fruhlinger, J. (2020). Marriott data breach FAQ: How did it happen and what was the impact? [online] CSO Online. Available at: <https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html>.
6. Google. (2022). Get to know the new Topics API for Privacy Sandbox. [online] Available at: <https://blog.google/products/chrome/get-know-new-topics-api-privacy-sandbox/>.
7. ICO (2019). Personal data breaches. [online] Ico.org.uk. Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>.
8. ico.org.uk. (2021). Some basic concepts. [online] Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-dpa-2018/some-basic-concepts/>.
9. Information Commissioner's Opinion: Data protection and privacy expectations for online advertising proposals. (2021). [online] Available at: <https://ico.org.uk/media/about-the-ico/documents/4019050/opinion-on-data-protection-and-privacy-expectations-for-online-advertising-proposals.pdf>.
10. Introduction to anonymisation Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance. (2021). [online] Available at: <https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf>.
11. ITRC. (2022). 2021 Annual Data Breach Report. [online] Available at: <https://www.idtheftcenter.org/publication/2021-annual-data-breach-report-2/> [Accessed 24 Apr. 2022].

12. Legislation.gov.uk. (2018). Data Protection Act 2018. [online] Available at: <https://www.legislation.gov.uk/ukpga/2018/12/section/34/enacted>.
13. Lucivero, F., Hallowell, N., Johnson, S., Prainsack, B., Samuel, G. and Sharon, T. (2020). COVID-19 and Contact Tracing Apps: Ethical Challenges for a Social Experiment on a Global Scale. *Journal of Bioethical Inquiry*, 17.
14. Meszaros, J. and Ho, C. (2021). AI research and data protection: Can the same rules apply for commercial and academic research under the GDPR? *Computer Law & Security Review*, 41, p.105532.
15. Narayanan, A. and Shmatikov, V. (2008). Robust De-anonymization of Large Sparse Datasets. 2008 IEEE Symposium on Security and Privacy (sp 2008). [online] Available at: https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf.
16. Rocher, L., Hendrickx, J.M. and de Montjoye, Y.-A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications*, 10(1).

Bibliography

1. Chico, V. (2018). The impact of the General Data Protection Regulation on health research. *British Medical Bulletin*, 128(1), pp.109–118.
2. Fahey, R. and Hino, A. (2020). COVID-19, digital privacy, and the social limits on data-focused public health responses. *International Journal of Information Management*, [online] 55, p.102181. Available at: <https://www.sciencedirect.com/science/article/pii/S0268401220310239>.
3. Kerry, C.F. (2020). *Protecting privacy in an AI-driven world*. [online] Brookings. Available at: <https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/>.
4. Meszaros, J. and Ho, C. (2021). AI research and data protection: Can the same rules apply for commercial and academic research under the GDPR? *Computer Law & Security Review*, 41, p.105532.
5. Oseni, A., Moustafa, N., Janicke, H., Liu, P., Tari, Z. and Vasilakos, A. (2021). Security and Privacy for Artificial Intelligence: Opportunities and Challenges. *arXiv:2102.04661 [cs]*. [online] Available at: <https://arxiv.org/abs/2102.04661>.
6. Pfarr, F., Buckel, T. and Winkelmann, A. (2014). *Cloud Computing Data Protection – A Literature Review and Analysis*. [online] IEEE Xplore. Available at: <https://ieeexplore.ieee.org/document/6759219> [Accessed 2 May 2022].
7. Rebello, C. and Tavares, E. (2018). Big Data Privacy Context: Literature Effects On Secure Informational Assets. *TRANSACTIONS ON DATA PRIVACY*, [online] 1, pp.1–21. Available at: <https://arxiv.org/pdf/1808.08537.pdf>.