Queen Mary
University of London

Report on the Marriott Data Breach

ECS7025P

Ethics, Regulation and Law in Advanced Digital Information Processing and Decision Making – 2021/22

Executive Summary

Whilst the right to data protection is closely related to the well-known right of privacy, there are distinct differences between the two which justify the former's eventual formulation as an independent right. The large-scale data collection projects carried out by governments in the 1960s - made possible by rapid technological advancements - created awareness that the traditional interpretations of personal privacy may be unable to cope with and protect against the dangers of the emerging informational dimension of the term. As a response, the following decades produced increasingly comprehensive data protection frameworks and regulations, such as the Privacy Act 1974, the two Resolutions of the Council of Europe (1973&74), the EU Data Protection Directive (DPD, 1995) or the General Data Protection Regulation (GDPR, 2018) - detailing the growing rights of individuals and obligations of data controllers with regard to data.

The large-scale data breach of Marriott International between 2014 and 2018, however, highlighted the fact that despite the progress made in legislation and general awareness regarding data protection, many companies still lag behind and fail their privacy safety duties by a large margin. Due to a combination of technical and organisational failures (e.g., inadequate monitoring of databases, lack of server hardening practises, or the inconsistent and missing encryption on data records), Marriott exposed an estimated 339 million guest records to cyber-criminals and was eventually fined for a staggering £18.4 by the UK's Informational Commissioner's Office (ICO).

The fine was based on two breached GDPR principles, namely 'Integrity and Confidentiality' and 'Security of Processing' – however, the case also underlined the importance of organisations adhering to ICO's Data Sharing Code (DSC, 2021) - specifically, its recommended due diligence practises around M&A transactions.

One can also relate the Transparency and Accountability Principles of the UK Data Ethics Framework (DEF, 2020) to the Marriott breach, as they were clearly inappropriately represented by the company. First, a clear and consistent internal security framework guiding the cyber-security division of Marriott with regard to safety measures, but also, raising awareness and stating explicit roles of all employees within the firm in terms of their security responsibilities. Second, the authorities' (e.g., ICO) oversight of Marriott's business operations and its security measures could have been tighter, better representing the public's interest, for example, through active collaboration with other leading authorities in the financial sector (e.g., auditing firms).

The increasing number of companies being fined for violating data protection laws indicate that complete avoidance of data breaches is not possible. Nonetheless, both authorities and organisations must strive towards cyber safety measures that reduce and/or mitigate the occurrences and depth of such data breaches. In relation to the Marriott case, this report offers three policy recommendations: (1) mandatory, comprehensive, regular, and uniform training provided to all organisations by the ICO, in order to level out financial differences between companies in acquiring training for their employees; (2) ICO's collaboration with other regulators and authorities in different fields (e.g., financial regulators or auditors directly in contact with companies), as to better harmonise its monitoring of firms' adherence to regulations; finally, (3) making personal data breaches a criminal act, which could induce organisations, specifically their executives, to take their obligations more seriously.

Table of Contents **Page**

List of Abbreviations

CDE – Cardholder Data Environment

CEO – Chief Executive Officer

CFO – Chief Financial Officer

CIO – Chief Information Officer

CoE – Council of Europe

DEF – Data Ethic Framework

DPA – Data Protection Act

DPAs – Data Protection Authorities

DPD – Data Protection Directive

DPIA – Data Protection Impact Assessment

DSC – Data Sharing Code

EEA – European Economic Area

FIP – Fair Information Practises

GDPR – General Data Protection Regulation

ICO – Informational Commissioner's Office

IP – Internet Protocol

Introduction

ICO (2022) defines data protection as part of the fundamental right to privacy, involving fair and transparent use of information about people. During the data protection process, preserving people's control over their identity and interactions with others are balanced with ensuring society's wider interests, for example fighting terrorism, criminality, or fraud. ICO states that such balancing is vital for inducing a general trust both in the private and public sectors for innovative uses of data or trade.

The cyber-attack on Marriott International's systems between 2014 and 2018, which resulted in a serious data breach, however, highlights the vulnerability of individuals and companies to both their own fallacies in protecting their data, and the malicious acts of cyber-criminals through which the abovementioned data protection balance can be broken. Consequently, it also shows the need for individuals, companies, and regulators to comply, strengthen, and advance the current state of privacy safeguards. Regulators and lawmakers must constantly adapt to the new techniques of criminals, whilst companies must go beyond merely complying with the minimum requirements of data protection regulations and actively build safety measures that are inherent to their very business fabrics.

Understanding the emergence, evolution, and eventual separation of the definition of data protection from the well-established rights of privacy can enlighten its significance and give context to the Marriott case analysed below. Section A, therefore, provides an overview of these concepts, through a brief literature review, which guides the reader through the cornerstones of privacy law regulations, including the FIP of Privacy Act 1974, the two Resolutions of the Council of Europe (CoE; 1973, 1974), the EU DPD (1995), and the GDPR (2018).

Section B provides critical analysis and discussion with regard to the Marriott case by reflecting on the various points the company deviated from the ICO DSC (2021), the Data Protection Act (DPA, 2018) and the GDPR, and examining which UK DEF (2020) Principles could be applied to understand the case. The analysis is based on primary research findings and an interview conducted with a Data Protection paralegal working at Google.

Section C draws insights to what measures could have been taken by Marriott to prevent the data breach, and simultaneously suggests policy recommendations to the ICO with reference to the Marriott case.

Section A – Literature Review

For the most part of history, privacy was related to the most intimate aspects of being human, such as one's property or family life. These aspects can be thought of as the relational dimension of privacy - one's relation with others – for example, who can enter one's house or touch one's body (Holvast, 2009). From the end of the 19th century, however, privacy law discussions slowly turned towards the control of one's personal information. For example, in "The Right to Privacy" (1980), Samuel Warren and Louis Brandeis defined privacy as the right to be let alone.

The rapid advancements of technology and the accompanying increased data collection of governments about their citizens in the 1960s, induced greater awareness that this aspect of privacy should be equivalently protected, thereby shifting the general discussion even further, towards privacy's informational dimension (Sloot, 2014). For instance, in 'Privacy and Freedom' (1967), Alan Westin defined privacy considering this new dimension: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (p. 7).

The Privacy Act of 1974 and its proposed Fair Information Practices (FIP) in the US was a pioneering legislation which recognised that the traditional view and dimension of right to privacy is unfit to the new challenges of large-scaled, automated personal data collecting and processing, primarily done by governments. Whilst the former gives a unilateral role to individuals in deciding the nature and extent to her self-disclosure, the latter realises that both individuals (subject of data records with the risks and implications associated with such processes) and institutions (data collectors using the personal data) might have different interests, but the purpose and benefit of data records is shared by both parties – e.g., protecting national security, or statistical analysis for effective social economic policy decisions (Sloot, 2014). The problem at hand, then, is one of balancing opposing interests: data subjects need safeguards against the invasion of their privacy (data abuse or disclosure) through objecting data collectors to specific obligations and giving certain rights to the data subjects, whilst ensuring institutions to use public data for the benefit of society (OECD, 2013).

The FIP were geared toward two general obligations: transparency and fairness. First, data collecting agencies had to publish annual notices for the public, containing the name, nature, and purpose of their database systems, with information about data storage, retention, and categories of maintained data, among others. Second, they restricted further processing or transfer of data to third parties; required adequate measures in place against data breaches; and set forth specific record-keeping requirements (DOJ, 2020). Subsequently, FIP also equipped

individuals with access to their personal data and provided marginal rights on rectification and erasure too.

In Europe, the CoE adopted two Resolutions with regard to data processing: one for the private (1973) and one for the public sector (1974). It recommended similar obligations for data controllers as the Privacy Act of 1974: principles to be undertaken by member states relating to obtaining data (fairly and lawfully), maintenance of data quality (stored securely and accurately, no longer than it is necessary; used for specified, legitimate purposes only), and rights to be given to individuals about their data (directed at the public in general) and the processing activities involved with it. The Convention of the CoE was accepted in 1980, which enforced the Resolutions among its member governments, and reduced data flow restrictions between its members by encouraging co-operation of the respective national data protection authorities (OECD, 2013).

The EU DPD (Directive 95/46/EC) adopted in 1995, made two important changes to Convention 1980. First, besides the controllers' continued obligation to notify the national Data Protection Authorities (DPAs) about their data processing activities, the duty of informing the public has been broadened to notify the data subject itself about the (i) identity of the controller, (ii) the purposes of the processing, and (iii) the recipients of the data (Sloot, 2014).

Second, the Directive specified that the only grounds for legitimate data processing are (i) consent from data subject, (ii) contractual requirement, (iii) legal obligation, (iv) protection of the interests of the data subject, (v) protection of the interest of the public, or when (vi) the interest of the controller exceed the data subject's.

The EU's GDPR was adopted in 2016 and became enforceable from 25 May 2018, superseding the DPD and becoming national law for all members of the EU. Whilst it builds on the principles of DPD, there are significant changes in its data protection requirements, scope, and enforcement. First, the interpretation of consent has been tightened, making the controller responsible to have proof for the data subject's consent (with special provision for children under the age of thirteen).

Second, besides the already known and accepted rules concerning fair and lawful processing and data quality by the Directive, controllers are expected to carry out accountability duties, including exact documentation of processing operations, carrying out data protection impact assessments, or appointing a data protection officer, among others.

Third, rather than notifying the supervisory authorities about the processing activities, companies are required to document all their data operations and notify the authorities only when a data breach has occurred. Controllers must also provide clear and easily accessible

information to the data subjects about their operations at all times, but only notify them directly if a potential data breach adversely affect their interests.

The evolution of the abovementioned data protection measures and privacy safeguards can be summarised with regard to the obligations of data processors, and the rights of data subjects. First, the annual notification of the public by the controllers, regarding their data operations have been replaced by the duty of the controller to have a transparent and accessible policy for its operations; and those subjects should only be notified in case of a significantly detrimental data breach. Whilst the principle of fairness (lawful, secure, confidential data processing with attention to data quality) have been remained largely unchanged, controllers' obligations have been extended by their accountability duties, providing adequate safety for the subjects' interests and personal information.

Second, data objects' rights have been strengthened substantially: their initially weak rights to accessing, rectifying, or erasing data, and some threshold-tied-objection against automatic decision making have been strengthened and expanded by the GDPR, which additionally equips them with the right of data portability, and the right to be forgotten.

Third, the initial rules were merely vague good governance practices, applied to the processing 'pipeline', rather than formulated explicitly as human rights of the individuals. This has eventually changed, when the Charter of Fundamental Rights of the European Union (2009) declared data protection a fundamental human right in Article 8, separately from the right to privacy. Violation of the data protection right entails specific monetary penalty fees.

In the following, Section B first defines what constitutes as personal data and breach, and the primary motivations behind them. It then briefly introduces the Marriott case, reflects on the four principal failures ICO found on behalf of Marriott in the data breach, then categorise these failures in terms of GDPR Articles and the ICO's DSC. Finally, it reviews the case through the lenses of two related principles of the UK DEF.

Section B – Research and Discussion

About Data Breaches and the Motivations Behind Them

Article 4 (1) GDPR defines personal data as "a name, identification number, location data, online identifier, or one or more factors specific to a data subject's physical, physiological, genetic, mental, economic, cultural, or social identity." Article 4 (12) describes personal data breaches as "a breach of security leading to the accidental or unlawful destruction, loss,

alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Holvast (2009) suggests that there are two important characteristics of information: power and money. These can ultimately be thought of as the motivations behind the personal data collection, storage, and use (e.g., data mining, at the end of which information is extracted from raw data) by companies and governments. But equivalently, they also provide the rationale for cyber-criminals to gain unauthorised access to such data. Placing this argument in the context of the Marriott data breach, the hotel chain collected personal data for business purposes (e.g., maximising revenue by analysing guests' data, from which loyalty programs could be created), whilst the cyber attackers stole information to either sell that data, or as indicated by many, was conducted as a nation-state intelligence-gathering operation for espionage purposes (NPR, 2018). Nonetheless, the occurrence of data breaches (including the Marriott case) can also be thought of taking place simply as a result of inadequate safety measures on the part of the data collector.

In brief, the ICO slapped an £18.4 fine on Marriott International Inc. due to the company's technical and organisational failures to protect personal data. The breach which originated in a 2014 cyber-attack on Starwood Hotels and Resorts Worldwide Inc.'s reservation system went undetected until September 2018, by which time Marriott acquired Starwood in 2016. An estimated 339 million guest records were exposed globally, of which approximately 30 million records related to countries in the EEA. The stolen records were personal in nature as they contained names, birth dates, credit card information, home addresses, and passport numbers, among others (Dasvani & Elbayadi, 2021).

Critical Issues

UK's ICO, the leading supervisory authority in the case, found four principal failures of Marriott. First, there was insufficient monitoring of privileged user accounts that could have detected the 2014 breach. The ICO argued in its Penalty Notice (2020) that their concern is not regarding the penetration of the attackers into Starwood's systems, but the lack of appropriate and adequate measures (e.g., logging) - primarily through sufficient monitoring of privileged user account activity - that could have detected and blocked further unauthorised activity of the attacker in the abovementioned privileged accounts.

Second, Marriott inadequately monitored its databases too, particularly its cardholder data environment (CDE). The ICO named three failures in this regard: (i) deficient security

alerts on databases of the CDE; (ii) lack of aggregating log files (allowing efficient monitoring of network activity); and (iii) inadequate logging of key operations on CDE systems, such as creation and export of database tables. Whilst logging and security alerts were partially implemented on tables that contained payment card information or specific queries, most operations of the attackers could go undetected, including exporting complete database tables, as such operations did not trigger the alerts.

Third, Marriott failed to carry out server hardening which could have prevented the attackers to gain access to privileged accounts or at least restrict their mobility once entered. ICO recommended the use of whitelisting of selected IP addresses or permitted software by the company, especially on critical systems containing significant amounts of personal data.

Fourth, other than on its payment-related records, encryption on Marriott's data was not applied, including passport numbers. Moreover, the encryption key used to encrypt and decrypt the credit card details were stored in the same database as the credit information, meaning that the attackers were likely able to decrypt the stolen data.

Marriott and the ICO's Data Sharing Code

Whilst not being in violation of the GDPR according to the ICO (in this specific case as it happened before GDPR came into force), Marriott failed to perform a sufficient due diligence procedure at the acquisition of Starwood. This would have involved obtaining security reviews and questionnaires from Starwood's IT management, carrying out penetration and hunting exercises by ethical hackers, in order to 'harden' the organisation's most vulnerable points (Dasvani & Elbayadi, 2021).

However, such practices, for example, Data Protection Impact Assessments (DPIAs) are heavily recommended by ICO's DSC (produced under the requirement of Section 121 of DPA 2018 by the ICO), which is aimed at guiding data controllers on how to exchange personal data among each other in a fair and lawful way. Non-compliance with the DSC will almost always result in violation of the GDPR and the DPA (ICO, 2020) – for instance, the data exchange during Marriott and Starwood's M&A is a illustrative case in point.

GDPR Articles Breached

Taking into account the abovementioned security issues detected in Marriott's system (but only considering those infringements that happened after GDPR came into force in May 2018), the ICO fined Marriott based on the violation of Article 5(1)(f) and Article 32 GDPR.

The former refers to the 'Integrity and Confidentiality' principle being violated, that is, processing data in a manner that prevents "unauthorised or unlawful processing and against accidental loss, destruction or damage" of personal data under care. The latter is about a 'Security of Processing', that is, security measures organisations must have which is appropriate for the risk to the data. Such measures could include the abovementioned encryption techniques, ensuring confidentiality, or testing security systems as an ongoing process.

Moreover, in its initial findings, ICO stated that Marriott also infringed Article 33 GDPR, regarding the 'Notification of a Personal Data breach to the Supervisory Authority'. This Article prescribes companies a 72-hour mandatory notification of breach. Eventually, this was not considered as a breach, but there was disagreement between the ICO and Marriott as to whether the data controller has to be reasonably certain that a breach had occurred before notifying the ICO. The ICO stated that the data controller "must be able to reasonably conclude that it is likely a personal data breach has occurred to trigger the notification requirement under Article 33" (Author).

Finally, although the Commissioner declared that Marriott did not breach Article 34 GDPR ('Communication of a Personal Data Breach to the Data Subject'), Marriott notification mechanism to the data subjects was insufficient. Rather than contacting each data subject individually (which could have been done, hence Marriott's lack of demonstration against it), Marriott set up a public website for inquiries and issued a press release.

Understanding the Marriott case through UK Data Ethic Framework's Principles

Whilst the UK DEF (2020) is directed at those working in the public sector in data-related positions, its principles can offer insights into what went wrong in Marriott's case, and potentially inspire private sector participants in the ways they organise their businesses.

DEF's Transparency principle proposes a clear and consistent framework, readily available for the public about the ways a public data-related project is carried out. A similar framework should have been place in Marriott's internal systems, guiding not only their cyber security personnel against the vulnerabilities of their systems (listed above as 'Critical Issues'),

but holistically all their employees across their departments. Whilst there were measures and safeguards present in Marriott's security plan, they were seemingly inconsistent and arbitrarily applied.

Second, DEF's Accountability principle states that representatives of the public should exercise effective oversight and control over governmental projects and decisions, guaranteeing that the promised social objectives are achieved. One could say that governmental authorities (e.g., the ICO) represent the interests of the public – in this case, their oversight seems to have been too lax. More stringent monitoring on their part, whilst involving the public directly to a greater extent by raising awareness around data protection could perhaps prevented the breach. According to Daswani and Elbayadi (2021), it seems that in Marriott's case, the company's business interests came into conflict with its GDPR obligations towards the public around the time Starwood's acquisition. They argue that Marriott's responses during the attacks and in terms of its overall security policies were rather reactive in nature, that is, complying with regulations (partially) as in ticking the boxes, but never fully achieving them or going beyond with proactive initiatives. In their interpretation, this might have been due to budgetary constraints, or lack of political and organisational support in the company. Consequently, the reason behind Marriott's failure to securely protect its data subjects' records, in light of DEF's Accountability principle, can be partially seen as the lack of accountability the company faced from the ICO.

Section C – Conclusion and Recommendations

Lessons learned

This paper considers three broad takeaways from the Marriott case. First, Marriott's data breach highlights the importance of giving priority and focus to cybersecurity considerations when merging or acquiring businesses. If a company acquires a breached organisation without sufficient vetting and due diligence procedures, the former becomes breached as well. The ICO's DSC offers a practical and clear guidance as of what necessary steps need to be taken to adequately review every aspect of the company that is being acquired, including a mixture of auditing, penetration tests, configuration reviews, or hunting exercises. Doing so will not only mitigate the risk of violating data protection regulations, but simultaneously guard against those potential violations' broader repercussions, such as loss of public trust in the brand, class lawsuits, and the accompanying hit in profits in the long run.

Second, it is clear from the emerging new cases in which companies are fined by regulators for breaching data regulation laws that, it is impossible to prevent all breaches. What is important is to make it harder to happen, or if they do happen, have measures and systems in place that contain and mitigate the damage - these systems must be clear, consistent throughout, and have multiple layers. The magnitude of the breach in Marriott's case was multiplied by the poor data management policies in place both at Starwood and Marriott. The lack of encryption (or where it was present, data stored was in the same database as the encryption key), limited monitoring and incident reports of databases and privileged user accounts, all point to inconsistencies in Marriott's policies and overall management.

Third, increased executive accountability is needed, including CEOs, CFOs, and CIOs. The previous two points both suggest that there was inadequate level of support for cybersecurity within and among Marriott's different divisions. For example, at the time of the breach, none of Marriott's board members had a technology or cybersecurity background, nor did the company have a dedicated cyber-risk committee (Dasvani & Elbayadi, 2021). Consequently, an organisation aiming to establish a comprehensive cybersecurity system should have people with appropriate backgrounds in positions where prioritisation of cybersecurity matters can be enforced or at least made aware of.

Policy Recommendations

Whilst the regulations of GDPR covers the obligations of organisations as entities in their entirety with regard to cybersecurity, it is likely that only a small fraction of a large corporation is aware of the dangers of cyber criminals. Of course, the ICO recommends training around security awareness and provides detailed guidance on how to meet their expectations, however, this report suggests that it should provide a mandatory and comprehensive training course itself, free of charge. This would eliminate differences in the course materials companies take, their varying quality (depending on what quality a company can afford) and ensure that they are actually carried out regularly throughout the organisations. The rationale behind this suggestion is that an organisation's security is only as strong as its weakest member – following the above logic, a poorer company's weakest member should not be less trained than a more affluent firm's.

Second, authorities could be more present in the monitoring of companies' adherence to safety measures and practises, increasing the organisations' accountability towards the public. As cybersecurity practises are likely to get loose or sacrificed during constrained

financial times of an organisation, ICO could collaborate with various other authorities in the financial sector (e.g., auditing firms), and harmonise its monitoring activities according to an organisation's financial situation.

Third, besides the welcomed increase in penalty fees upon data protection violations, perhaps making personal data breaches a criminal act could also induce organisations, specifically their executives, to take their obligations more seriously.

Role of UK ICO and Awareness of People

The ICO is the UK's data protection watchdog responsible for enforcing compliance with regulations regarding data protection, networking, or communication regulations, including the GDPR and the DPA 2018. Among its roles and responsibilities are the investigation of breached organisations, executing spot-checks of their compliance, or issuing information notices and/or penalties where needed (Afifi-Sabet, 2021). They are also in place to uphold rights in the public interest, promote openness by public bodies and data privacy for people.

The general awareness of companies and the public about data protection and the value of personal data has definitely increased over the years, probably due to large companies being fined over breaches with extensive media coverage (e.g., Facebook, Google, or British Airways). However, additionally, different age generations could be targeted differently to engage with the ICO – for example, talks could be organised at high schools about the importance and value of personal data, or games created around the topic on social media platforms. For older generations, besides the abovementioned idea of mandatory training courses for professionals, ICO could be more present in newspaper articles, or on TV shows.

Bibliography

Afifi-Sabet, K. (2021). What is the Information Commissioner's Office (ICO)?. *ITPro. Available at: https://www.itpro.co.uk/information-commissioner/31751/what-is-the-information-commissioner-s-office-ico [Accessed: 23/4/2022]*

Charter C326/391. (2012). Charter of Fundamental Rights of the European Union. *Official Journal of the European Union, C 326/391. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN [Accessed: 21/4/2022]*

CoE Resolution. (1973). Council of Europe Committee of Ministers - Resolution (73) 22 On the Protection of the Privacy of Individuals Vis-à-vis Electronic Banks in the Private Sector. (Adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies). *Available at: https://www.mybib.com/tools/harvard-referencing-generator [Accessed: 20/4/2022]*

CoE Resolution. (1974). Council of Europe Committee of Ministers – Resolution (74) 29 On the Protection of the Privacy of Individuals Vis-à-vis Electronic Data Banks in the Public Sector. (Adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies). *Available at: https://rm.coe.int/16804d1c51 [Accessed: 20/4/2022]*

Daswani, N., Elbayadi, M. (2021). Big Breaches: Cybersecurity Lessons for Everyone. *Apress, ISBN:* 9781484266557.

Data Protection Act. (2018). Data Protection Act 2018. [online] GOV.UK. *Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted [Accessed: 20/4/2022]*

DEF. (2020). Data Ethics Framework 2020. [online] GOV.UK. *Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/923108/Data_Ethics_Framework_2020.pdf [Accessed: 19/4/2022]*

DOJ. (2012). Overview of the Privacy Act - The Privacy Act of 1974, 5 U.S.C. § 552a (2012). *U.S. Department of Justice Office of Privacy and Civil Liberties. Available at: https://www.justice.gov/archives/opcl/page/file/844481/download [Accessed: 21/4/2022]*

Donn, P. (2020). The data breach that cost Marriott £18.4 million – what went wrong? *Data Protection Network. Available at: https://dpnetwork.org.uk/data-breach-costs-marriott-18-million/ [Accessed: 21/4/2022]*

DPD - 95/28/EC. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN [Accessed: 20/4/2022]*

DSC. (2021). Information Commissioner's Office - Data sharing code of practice. *Available at: https://ico.org.uk/media/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice-1-0.pdf [Accessed: 19/4/2022]*

GDPR. (2018). Guide to the General Data Protection Regulation. [online] GOV.UK. *Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf [Accessed: 20/4/2022]*

Hewson, K., Sigler, B. (2020). An analysis of the Monetary Penalty Notice issued by the Information Commissioner's Office to Marriott International, Inc. dated 30 October 2020. *Stephenson Harwood. Available at: https://www.shlegal.com/news/an-analysis-of-the-monetary-penalty-notice-issued-by-the-information-commissioner-s-office-to-marriott-international-inc.-dated-30-october-2020 [Accessed: 22/4/2022]*

Holvast, J. (2009). History of privacy. In V. Matyáš, S. Fischer-Hübner, D. Cbrček, & P. Švenda (Ed.), *The Future of Identity in the Information Society (pp. 13-42). Berlin: Springer.*

ICLG. (2021). Data Protection Laws and Regulations – The Rapid Evolution of Data Protection Laws (2021-2022). *Available at: https://iclg.com/practice-areas/data-protection-laws-and-regulations/1-the-rapid-evolution-of-data-protection-laws [Accessed: 23/4/2022]*

ICO. (2020). Information Commissioner's Office – Penalty Notice, Section 155, Data Protection Act 2018, Case ref: COMo8o4337. *Available at: https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf [Accessed: 22/4/2022]*

Kirsop, J., Davey, S. (2020). Marriott and BA: cybersecurity basics emphasised in GDPR enforcement. *Pinsent Masons. Available at: https://www.pinsentmasons.com/out-law/analysis/marriott-ba-cybersecurity-gdpr-enforcement [Accessed: 22/4/2022]*

Lord, N. (2018). What is the Data Protection Directive? The Predecessor to the GDPR. *Data Insider – Digital Guardian's Blog. Available at: https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr [Accessed: 22/4/2022]*

McDermott, Y. (2017). Conceptualising the right to data protection in an era of Big Data. *Big Data & Society, Vol. 4, No. 1, pp. 1-7.*

OECD. (2012). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Available at: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [*Accessed: 21/4/2022]*

Schwartz, M.J. (2020). Probing Marriott's Mega-Breach: 9 Cybersecurity Takeaways. *Bank Info Security. Available at: https://www.bankinfosecurity.com/probing-marriotts-mega-breach-9-cybersecurity-takeaways-a-15338. [Accessed: 20/4/2022]*

Scroxton, A. (2020). What can we learn from Marriott's new data breach embarrassment. *ComputerWeekly. Available at: https://www.computerweekly.com/news/252481000/What-we-can-learn-from-Marriotts-new-data-breach-embarrassment [Accessed: 23/4/2022]*

Van der Sloot, B. (2014). Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation. *International Data Privacy Law, Vol. 4, No. 4., pp. 307-325.*

Warren, S.D., Brandeis, L.D. (1890). The Right to Privacy. *Harvard Law Review, Vol. 4, No. 5., pp. 193-220.*

Westin, A.F. (1967). Privacy and Freedom. *Atheneum, New York.*

Wilhelm, E-O. (2016). A brief history of the General Data Protection Regulation (1981-2016). *iapp. Available at: https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/ [Accessed: 18/4/2022]*

Wynn, K. (2020). Data sharing code expands ICO's views on M&A data due diligence. *Pinsent Masons. Available at: https://www.pinsentmasons.com/out-law/news/data-sharing-code-ico-ma-due-diligence [Accessed: 23/4/2022]*

Young, K. (2021). Cyber Case Study: Marriott Data Breach. *Coverlink Insurance. Available at: https://coverlink.com/case-study/marriott-data-breach/ [Accessed: 21/4/2022]*