Journal of Legal Subjects
ISSN: 2815-097X
Vol : 03 , No. 04 , June-July 2023
http://journal.hmjournals.com/index.php/JLS
DOI: https://doi.org/10.55529/jls.34.32.41

Data Privacy Regulations in Ghana: A Guide to GDPR Compliance for Businesses

Zimpah Bikunati Joseph[1*], Kwabena Boateng Mensah[2], Zimpah Nafah Abraham[3]

[1]Wisconsin International University College Ghana.*
[2]Academic City University, Ghana.
[3]Zimpah Foundation LBG, Ghana.

Corresponding Email: [1]josephzimpah@gmail.com*

Received: 27 March 2023 **Accepted:** 13 June 2023 **Published:** 29 July 2023

Abstract: ***The protection of personal data is a top priority for both individuals and organizations in the modern digital world. In the Ghanaian context, strict data privacy laws are essential to protecting citizens' rights and privacy. The legal foundation for these restrictions is the 1992 constitution of Ghana and Data Protection Act, specifically the Data Protection Act, 2012 (Act 843), which establishes the guidelines for legitimate data processing, the responsibilities of data controllers and processors, and the rights of data subjects. Compliance with local laws, however, may not be sufficient for enterprises operating on a worldwide scale or in international marketplaces as a result of the fact that globalization and digitalization cut across national boundaries. This article delves into Ghana's complex data privacy landscape, illuminating key points and providing suggestions for how businesses can improve their data protection practices by adhering to internationally recognized data protection standards like the General Data Protection Regulation (GDPR) of the European Union. Understanding the fundamental principles of Ghana's Data Protection Act, the scope and applicability of GDPR in Ghana, the importance of data mapping and inventory, the function of Data Protection Impact Assessments (DPIAs), consent and the rights of data subjects, data security and breach notification, and the potential sanctions for non-compliance are some of the key areas of focus. Readers can obtain a profound awareness of Ghana's data privacy landscape and the procedures necessary to successfully align with national and international data protection regulations by navigating this in-depth exploration. Businesses that prioritize compliance with data protection regulations in Ghana are better positioned not only to meet legal requirements but also to foster trust, drive innovation, and contribute to the nation's digital advancement on the global stage. In an ever-evolving digital world where data privacy is paramount.***

Keywords: ***Data Privacy Regulations, Ghana Data Protection Act, GDPR Compliance, Data Protection Commission.***

Journal of Legal Subjects
ISSN: 2815-097X
Vol : 03 , No. 04 , June-July 2023
http://journal.hmjournals.com/index.php/JLS
DOI: https://doi.org/10.55529/jls.34.32.41

1. INTRODUCTION

The protection of personal data is becoming increasingly crucial for both individuals and enterprises in the modern digital world. Data privacy laws are essential to protecting citizens' rights and privacy in Ghana, as they are in many other nations. The Data Protection Act, which outlines the requirements for legitimate data processing, the obligations and rights of data controllers and processors, and the rights of data subjects, serves as the cornerstone of these regulations.

Following local laws alone is typically insufficient in an increasingly interconnected world. Businesses that connect to global markets or conduct business globally may think about adhering to stricter, universally accepted data protection requirements. The General Data Protection Regulation (GDPR), which was put into effect by the European Union, is one such instance. Although Ghana has its own data protection regulations, companies there can successfully abide by both national and international data privacy standards by following the GDPR compliance guidelines.

In this article, we'll look at the specifics of Ghanaian data privacy regulations and discuss how businesses may employ GDPR compliance guidelines to fortify their data protection practices. We will examine key elements of the GDPR as well as Ghana's Data Protection Act, emphasizing their significance and applicability. Readers will have a solid understanding of Ghana's data privacy landscape at the end of this inquiry, as well as the steps necessary to successfully navigate it while upholding international standards.

Understanding Ghana's Data Protection Act

The Data Protection Act, 2012 (Act 843) is the primary piece of legislation governing data privacy in Ghana. By providing guidelines for how data controllers and processors may collect, store, use, or disclose personal information as well as by requiring adherence to particular data protection principles, the Act aims to protect people's privacy and personal data. The following are the key provisions of Ghana's Data Protection Act:

- Every department and agency within the Ghanaian government is subject to the Act's provisions.
- The Act governs the handling of personal data that comes entirely or partially from Ghana. By requiring a data controller or processor to process (collect, use, disclose, erase, etc.) such personal data or information in accordance with the individual's rights, the Act recognizes a person's right (data subject rights) to protect their personal data or information.
- The Act lays forth the regulations and guidelines for how a data controller or processor may acquire, use, disclose, and maintain personal data or information.
- The Data Protection Commission is a standalone statutory entity created by the Act to monitor and enforce compliance.
- Data controllers must register with the under the Act.

By complying with the key provisions of the Data Protection Act, businesses in Ghana can ensure they are protecting the privacy and personal data of individuals and meeting international data privacy standards.

Journal of Legal Subjects
ISSN: 2815-097X
Vol : 03 , No. 04 , June-July 2023
http://journal.hmjournals.com/index.php/JLS
DOI: https://doi.org/10.55529/jls.34.32.41

Scope of GDPR in Ghana

Under the General Data Protection Regulation (GDPR), the European Union (EU) has updated and harmonized its data privacy regulations. The GDPR defines a variety of goals, critical definitions, fundamental principles, and rights for data subjects in addition to requirements and sanctions for controllers and processors. Ghana is not, however, immediately impacted by GDPR.

The major piece of legislation governing data privacy in Ghana is the Data Protection Act, 2012 (Act 843). The Act regulates how data controllers and data processors receive, keep, use, or disclose personal information by requiring adherence to particular data protection standards. All individuals and organizations in Ghana are subject to the Act, and personal data is processed in a way that complies with the law, is reasonable, and doesn't infringe on the privacy rights of data subjects. In contrast, when processing data that is wholly or partially from Ghana, data controllers and processors are governed by the country's laws.

Using GDPR compliance guidelines, businesses in Ghana may make sure they are abiding by international data privacy laws. Businesses must obtain explicit consent from data subjects, process data for predetermined goals, confirm data correctness, impose a storage limit on data, and implement the required security precautions for personal data in order to be in compliance with GDPR. By following these suggestions, businesses in Ghana may make sure they are GDPR compliant and preserving international norms for data protection. It is important to keep in mind that Ghana does not have a law mandating adherence to the GDPR.

Data Mapping and Inventory

Data inventory and mapping are crucial components of data protection laws like the GDPR. Data mapping includes locating, gathering, and organizing various data across systems, keeping track of the data sources, and mapping the organization's data assets' storage and distribution patterns. Data inventory, on the other hand, aids in the mapping of how data is held and exchanged by identifying personal data within systems. According to Ghana's Data Protection Act, data controllers must register with the commission before processing any personal data. Businesses in Ghana can comply with the Act and make sure they are safeguarding customer data and privacy by using data mapping and inventory. Additionally, by developing a data map and inventory, businesses in Ghana can abide by international data protection regulations like the GDPR. Although it is not mandated by law in Ghana, business owners can apply GDPR compliance guidelines to make sure they are following international data privacy standards. Businesses must obtain explicit consent from data subjects, process data for predetermined goals, confirm data correctness, impose a storage limit on data, and implement the required security precautions for personal data in order to be in compliance with GDPR. Overall, data mapping and inventory are essential tools for companies in Ghana to utilize to ensure that they are protecting customer personal information and complying with data privacy rules.

Data Protection Impact Assessments (Dpias)

Data Protection Impact Assessments (DPIAs) are a part of key data privacy rules like the GDPR. DPIAs are designed to help businesses evaluate, identify, and reduce the data protection risks involved with a project or plan carefully. DPIAs are an essential part of the GDPR's

Journal of Legal Subjects
ISSN: 2815-097X
Vol : 03 , No. 04 , June-July 2023
http://journal.hmjournals.com/index.php/JLS
DOI: https://doi.org/10.55529/jls.34.32.41

accountability requirements and help businesses assess and demonstrate that they are meeting all of their data protection commitments.

DPIAs are required where processing puts a person's rights and freedoms at serious danger. DPIAs are required when processing sensitive data on a big scale, conducting in-depth assessments of an individual's personal traits, or routinely keeping an eye on public areas. DPIAs should be finished prior to processing, and they should be seen as a live tool rather than a one-time activity. For the DPIA, organizations can use the provided templates or develop their own unique ones that should be flexible and scalable.

There should be a level of rigor proportionate to the privacy issues involved, even though completing a DPIA doesn't always have to be challenging or time-consuming. Risks to compliance as well as greater threats to people's rights and freedoms, like the potential for any major social or economic harm, should be considered in DPIAs. The fundamental worry is the potential for harm whether physical, material, or non-material—to individuals or to society as a whole. Overall, DPIAs are an important tool for organizations to ensure they are complying with data privacy regulations, protecting the privacy and personal data of individuals, and minimizing data protection risks.

Consent and Data Subjects' Rights

The rights of data subjects and the importance of consent are both emphasized heavily in both the GDPR and the Ghanaian Data Protection Act. Here are some key concepts regarding consent and data subject rights:

1. Consent: Under Ghana's Data Protection Act, processing personal information without the subject's consent is prohibited unless required by law, permitted by a contract to which the subject is a party, required to protect the subject's legitimate interests, or necessary for the proper performance of a statutory duty. The GDPR requires that companies obtain the explicit agreement of data subjects before processing their personal information, which is similar to this.
2. Rights of data subjects: The Ghanaian Data Protection Act recognizes the right of an individual to protect their personal information by requiring a data controller or processor to handle that information in line with that person's rights. The right of data subjects to access their personal information, request that their personal information be made available, and file complaints with the Data Protection Commission. Similar to other privacy laws, the GDPR gives data subjects the right to access their personal information, correct any inaccuracies, request erasure, restrict processing, request data portability, and object to processing.
3. Businesses in Ghana may make sure they are safeguarding the privacy and personal data by adhering to these requirements.

Data Security and Breach Notification

Important components of data privacy rules include data security and breach notification. The following are some crucial details about data security and breach notification: a loss of data.

1. National notification standard for data breaches: The Personal Data Notification & Protection Act is a federal data breach notification requirement in the United States that

Journal of Legal Subjects
ISSN: 2815-097X
Vol : 03 , No. 04 , June-July 2023
http://journal.hmjournals.com/index.php/JLS
DOI: https://doi.org/10.55529/jls.34.32.41

seeks to improve data security by requiring that people and law enforcement receive notice when sensitive personal data is compromised.

2. State laws requiring consumer notification of security breaches: In the US, all 50 states have passed laws requiring consumer disclosure of security breaches when their personal information is compromised. These laws vary from state to state, but they often require businesses to notify anyone affected by a data breach right away.
3. HIPAA Breach Notification Rule: When unsecured protected health information is compromised, the HIPAA Breach Notification Rule requires that the impacted individuals, the Secretary of Health and Human Services, and, in some cases, the media be notified.
4. Data breach response guide: The Federal Trade Commission offers businesses a data breach response GUIDE that details actions to take in the event of a data breach. These actions include securing physical areas that may be connected to the breach, figuring out the applicable laws, and providing credit monitoring or identity theft protection services to affected individuals.
5. Businesses may make sure they are safeguarding customer information and privacy by adhering to these rules and regulations. They can also make sure they are responding appropriately in the event of a data breach.

Data breach response guide: The Federal Trade Commission offers businesses a data breach response GUIDE that details actions to take in the event of a data breach. These actions include securing physical areas that may be connected to the breach, figuring out the applicable laws, and providing credit monitoring or identity theft protection services to affected individuals.
Businesses may make sure they are safeguarding customer information and privacy by adhering to these rules and regulations. They can also make sure they are responding appropriately in the event of a data breach.

Penalties for Non-Compliance in Ghana

The penalties for breaking Ghana's data privacy regulations are laid forth in the Data Protection Act, 2012 (Act 843). A data controller or processor that breaks the law faces a fine of up to 150 penalty units, or GHS 3,000 or roughly $500 USD.
In addition to financial fines, breaching data privacy regulations may also result in reputational injury, a loss of customer trust, and legal action. Due to this, it is essential for businesses in Ghana to take data privacy legislation seriously and to take all necessary steps to ensure compliance. To avoid penalties for noncompliance, businesses in Ghana should adhere to the data protection regulations outlined in the Data Protection Act. Along with data security safeguards, data accuracy, and the data subject's participation. The appropriateness of processing, the articulation of the purpose, accountability, transparency, and compatibility of the following processing with the original goal of collection. Unless doing so is required by law, is necessary to uphold the terms of a contract to which the data subject is a party, or is necessary to protect the data subject's legitimate interests, businesses should make sure to obtain the consent of the data subject before processing any of their personal information.
In general, businesses in Ghana should take data privacy standards seriously and make sure they are adhering by all relevant laws and regulations in order to avoid penalties for non-compliance.

Journal of Legal Subjects
ISSN: 2815-097X
Vol : 03 , No. 04 , June-July 2023
http://journal.hmjournals.com/index.php/JLS
DOI: https://doi.org/10.55529/jls.34.32.41

The Telecos and Data Protection in Ghana

The Data Protection Act, 2012 (Act 843) is a law that must be complied with by all telecommunications providers operating in Ghana, including MTN. Except in certain situations, such as when the processing is necessary to fulfill a contract to which the data subject is a party, authorized or required by law, to protect a legitimate interest or pursue a legitimate interest of the data controller or a third party to whom the data is supplied, the Act requires data controllers who intend to process personal data to register with the Data Protection Commission and obtain prior consent from the data subject. Additionally, the Act gives data subjects the option of the National Communication Authority is in charge of overseeing the Ghanaian telecommunications industry, which includes issuing licenses to and policing telecom system providers, as well as assigning or allocating system frequencies.

However, it appears that the NCA is failing to keep an eye on Ghana's telecommunications industry. Mobile data and user privacy under the 2012 Data Protection Act. In Ghana, data protection is regulated under the Data Protection Act, 2012 (DPA), in conjunction with Article 18(2) of the 1992 Constitution, which grants citizens a fundamental right to privacy.

Enid Baaba Dadzie, a Senior Associate at Kimathi & Partners in Ghana, notes that the field of data protection is relatively new in Ghana, and there haven't been recent legal developments of note. However, she points out that the regulator in Ghana has been engaging in discussions with counterparts in other African countries. These discussions aim to consolidate and harmonize data protection laws, fostering the adoption of standardized data protection legislation across the continent. This collaborative effort is prompted by the emerging discussions surrounding data sovereignty, economization, and data localization.

Dadzie adds, "The regulator in Ghana is also pushing for data protection certification to become a requirement for businesses operating in Ghana. Additionally, discussions are underway with key individuals in Ghana to establish a dedicated data/cyber court capable of swiftly handling the growing cases of data breaches and cybercrime. Furthermore, the regulator has previously published the names of individuals and entities not in compliance with the DPA in newspapers, and it has recently intensified its enforcement efforts related to the DPA." These developments signify a growing commitment to data protection and privacy in Ghana, reflecting the broader international trend of strengthening data security and regulation. It's interesting to note that the Data Protection Act, 2012, Act 843, Chapter 20(1) expressly states: "A person shall not process personal data without the prior consent of the data subject, unless the purpose for which the personal data is processed is necessary for the purpose of a contract to which the data subject is a Unfortunately, it appears that important Ghanaian telecommunications providers including MTN, Vodafone, and Airteltigo either are not aware of the Data Protection Act, 2012, or purposefully and flagrantly ignore its terms. They keep using the mobile data of their clients without getting the required approval for marketing campaigns. In certain cases, they even reveal the mobile data of their clients to outside parties without their consent. Such behavior is not only offensive to and demoralizing for customers, but it also clearly against the law.party, authorized or required by law, to protect a legitimate interest of the data subject, necessary for the proper performance of a statutory duty; or necessary to:

Journal of Legal Subjects
ISSN: 2815-097X
Vol : 03 , No. 04 , June-July 2023
http://journal.hmjournals.com/index.php/JLS
DOI: https://doi.org/10.55529/jls.34.32.41

According to Chapter 20(2), "Unless otherwise provided by law, a data subject may object to the processing of personal data." The statement adds more evidence in favor of this. Worse still, this breach has led to dire consequences, including the hacking of personal information by fraudsters and the duping of unsuspecting clients of telecommunication companies, particularly in the surge of mobile money fraud. Despite customer complaints about these infringements on their data privacy, the telecommunication companies have largely ignored their concerns. The repercussions are far-reaching, with many individuals refusing to register their SIM cards with accurate personal information, thus undermining the government's commitment to trace every mobile number to its user. Instead, individuals resort to purchasing already registered SIM cards. Additionally, personal information and data are shared with Value Added Service (VAS) providers, who sometimes deceptively charge telecommunication company customers for services they did not subscribe to. This raises a crucial issue: Who monitors and controls these communications businesses' operations? In 1996, a parliamentary act created the National Communication Authority (NCA), which was responsible with policing the telecommunications industry and fostering efficient and fair competition. Even while the NCA has performed its duties admirably, it doesn't seem to be able to adequately oversee the actions of telecommunications firms in Ghana.

Telecommunications businesses are required by law to protect customer data submitted during SIM card registration. Only with the data subject's express consent may this information be processed and utilized. Unfortunately, it appears that the opposite is taking place, with personal information frequently entering the public domain. We are all susceptible to online fraud because a quick search on the internet can turn up a wealth of personal information.

While telecommunications firms have greatly increased socioeconomic activity in Ghana and helped to address the unemployment problem, they urgently need to take precautions to protect their clients and employees. In order to comply with the law and protect mobile data, data protection should be central to their business practices.

Emerging Trends and Challenges

Emerging Trends:

1. Ghana is currently undergoing a significant digital change, and this trend is anticipated to continue. As a result, there will be more data created and analyzed. Governments may be able to make better policy decisions with the help of effective data use.

2. Cloud-Powered Data Protection Services: Cloud-Powered Data Protection Services are becoming increasingly popular in Ghana. According to projections, 74% of enterprises would use these services by 2025, indicating an increasing reliance on cloud solutions for data security.

3. Economic Opportunities: There are a ton of new economic opportunities for Ghanaian companies thanks to the booming digital economy in West Africa. Businesses can take advantage of these chances as digital technologies advance to stimulate growth and innovation.

Pressing Challenges:

1. **Protection Gaps:** A significant number of organizations in Ghana still have considerable protection gaps in their data security infrastructure. These vulnerabilities expose them to

Journal of Legal Subjects
ISSN: 2815-097X
Vol : 03 , No. 04 , June-July 2023
http://journal.hmjournals.com/index.php/JLS
DOI: https://doi.org/10.55529/jls.34.32.41

the risks of cyberattacks and data breaches, highlighting the urgent need for robust protection measures.

2. **Ransomware Attacks:** Ransomware attacks have emerged as a looming threat in Ghana. An alarming 85% of organizations have reported at least one ransomware attack within the past year, emphasizing the critical importance of bolstering defenses against this type of cyber threat.
3. **Compliance Hurdles:** Achieving compliance with data privacy regulations remains a persistent challenge for businesses in Ghana. Particularly noteworthy is the increased vigilance of the Data Protection Commission in enforcing the Data Protection Act, underscoring the urgency of stringent compliance measures.
4. **Cross-Border Data Transfers:** The complexities surrounding cross-border data transfers are a recurring obstacle for Ghanaian businesses. Navigating the various legal frameworks governing such transfers poses significant compliance challenges, necessitating careful consideration and adherence.
5. **Cybersecurity Imperatives:** With the escalating menace of cybercrime and data breaches, businesses in Ghana face an imperative to fortify their cybersecurity defenses. Robust cybersecurity measures are essential to safeguard personal data and mitigate the risks associated with data breaches.

4. CONCLUSION

In today's digital age, data privacy has become an imperative concern, not only for individuals but also for businesses operating in Ghana. The framework for safeguarding personal data in the country is primarily outlined in the Data Protection Act, 2012 (Act 843), which delineates the rules governing lawful data processing, the roles and obligations of data controllers and processors, and the rights of data subjects.

However, as the globe becomes more interconnected, observing only local laws may not be enough, particularly for enterprises operating in foreign markets or on a worldwide scale. The General Data Protection Regulation (GDPR) of the European Union, for example, aligns with internationally recognized data protection norms in this regard. While Ghana continues to uphold its own stringent data protection regulations, adopting GDPR compliance guidelines can assist businesses in efficiently aligning with both national and international data privacy standards. Our investigation into Ghana's data privacy laws has brought to light a number of crucial components:

Understanding Ghana's Data Protection Act: The Data Protection Act, 2012 (Act 843), serves as the cornerstone of data privacy in Ghana. It establishes principles that govern the acquisition, usage, and disclosure of personal information by data controllers and processors, with the ultimate goal of protecting individuals' privacy rights. It also institutes the Data Protection Commission as a pivotal body responsible for enforcement.

Scope of GDPR in Ghana: While the GDPR itself does not have direct application in Ghana, its principles can be instrumental in ensuring international data privacy standards are met. Ghana's Data Protection Act, designed to apply to all individuals and agencies within the

Journal of Legal Subjects
ISSN: 2815-097X
Vol : 03 , No. 04 , June-July 2023
http://journal.hmjournals.com/index.php/JLS
DOI: https://doi.org/10.55529/jls.34.32.41

country, is sensitive to data originating partly or wholly from Ghana, aligning with the GDPR's territorial scope.

Data Mapping and Inventory: Effective data mapping and inventory are essential for compliance with data privacy regulations. These practices involve identifying, organizing, and understanding the flow of personal data within an organization. In Ghana, they are pivotal not only for compliance with the Data Protection Act but also for aligning with global standards, such as those set by the GDPR.

Data Protection Impact Assessments (DPIAs): DPIAs are indispensable tools for systematically assessing and mitigating data protection risks. These assessments are mandated when processing poses a high risk to individuals' rights and freedoms. DPIAs are not one-off exercises; they are living tools that adapt to evolving data protection requirements.

Consent and Data Subjects' Rights: Both the Data Protection Act in Ghana and the GDPR emphasize the importance of obtaining consent from data subjects before processing their personal data. Additionally, they grant data subjects rights that include access, rectification, erasure, and more, ensuring individuals have control over their data.

Data Security and Breach Notification: Ensuring robust data security and promptly notifying authorities and affected parties in case of data breaches are critical components of data protection regulations. Ghanaian businesses must follow these guidelines to protect individuals' data and maintain trust.

Penalties for Non-Compliance: Non-compliance with data privacy regulations in Ghana can result in monetary fines and reputational damage. Adherence to data protection principles outlined in the Data Protection Act is essential to avoid such penalties.

Ghana's data privacy landscape is evolving rapidly, with local regulations providing a solid foundation for safeguarding personal data. However, the globalized nature of data necessitates businesses to consider international standards, such as the GDPR, as valuable references for aligning with broader data protection principles. By comprehending the nuances of data privacy in Ghana, embracing GDPR compliance where applicable, and consistently adhering to best practices, businesses can navigate this intricate terrain successfully. Doing so not only safeguards the privacy of individuals but also fosters trust, promotes innovation, and contributes to Ghana's digital progress on a global stage. As the digital landscape continues to evolve, businesses must remain vigilant, adapt to emerging trends and challenges, and prioritize data protection as a fundamental aspect of their operations in Ghana and beyond.

5. REFERENCES

1. The 1992 Constitution of Ghana.
2. Botha, Johnny, et al. "A high-level comparison between the South African Protection of Personal Information Act and international data protection laws." ICMLG2017 5th International Conference on Management Leadership and Governance. 2017.

Journal of Legal Subjects
ISSN: 2815-097X
Vol : 03 , No. 04 , June-July 2023
http://journal.hmjournals.com/index.php/JLS
DOI: https://doi.org/10.55529/jls.34.32.41

3. Bellan, Maurice. "Juan Carlos Baker." 2019
4. Baako, Issah, Sayibu Umar, and Prosper Gidisu. "Privacy and security concerns in electronic commerce websites in Ghana: a survey study." International Journal of Computer Network and Information Security 11.10 (2019): 19.
5. Dagbanja, Dominic N. "The right to privacy and data protection in Ghana." African data privacy laws (2016): 229-248.
6. Reding, Viviane. "The European data protection framework for the twenty-first century." International Data Privacy Law 2.3 (2012): 119-129.
7. Act, Data Protection. "sections 24 https://nita. gov. gh/theevooc/2017/12." Data-Protection-Act-2012-Act-843. pdf (2012).
8. Berman, Gabrielle, James Powell, and Manuel Garcia Herranz. "Ethical considerations when using social media for evidence generation." (2018).
9. Costa, Angelo, et al. "A legal framework for an elderly healthcare platform: A privacy and data protection overview." Computer law & security review 33.5 (2017): 647-658.
10. Koops, Bert-Jaap. "The trouble with European data protection law." International data privacy law 4.4 (2014): 250-261.
11. Soegoto, D. S., and D. A. Oktady. "Information System Design of an Inventory Online Website." IOP Conference Series: Materials Science and Engineering. Vol. 407. No. 1. IOP Publishing, 2018.
12. Wahab, Magd Abdel, et al. "IOP conference series: materials science and engineering." (2019).
13. Jay, Rosemary, et al. Guide to the General Data Protection Regulation. London: Sweet & Maxwell, 2017.
14. Schwartz, Paul M., and Edward J. Janger. "Notification of data security breaches." Mich. L. Rev. 105 (2006): 913.
15. Regulation, General Data Protection. "General data protection regulation (GDPR)." Intersoft Consulting, Accessed in October 24.1 (2018).