


# Collaborative Discussion 2

## Initial Post



Initial Post

by Sahr Solar Sumana - Saturday, 27 January 2024, 11:18 PM

Upon the implementation of the UK GDPR there has been a tighter approach taken on how organisations handle personal data, thus reducing the risk posed to individuals as "personal data is any information that relates to an identified or identifiable living individuals" (European Commission, 2024).

Since UK GDPR is a domestic law that organisations must comply with, the Information Commissioners Office (2024) state that "the principles are broadly the same as those in the UK GDPR, and are compatible so you can manage processing across the two regimes". The processing of data for its required use is a key aspect of data wrangling, as part of the ICO's principles it is advised for processing activities to be documented alongside the business function the processing activity is the most applicable to. Whereas, UK GDPR requires that you do not have to document this sort of information, UK GDPR states that processing of data should be "lawful and necessary for the purposes and legitimate interests pursued by the controller and necessary for the performance of the required task" (Intersoft Consulting, 2023). In this case the ICO's data processing rule seems to be an extension or an additional layer of the UK GDPR law.

Since the Internet of Things (IoT) is rapidly expanding and entering the daily processes of public and private organisations, there needs to be a response to this within the sector of compliance "which is constantly evolving in response to new and ever-expanding breaches and attempts to secure protected data" (CompTIA, 2016). This additional layer provided by the ICO allows the rule on the use of personal data processing to have a form of contextual guidance allowing the law set out by the UK GDPR to be easily applied to current and future potential breaches.

References:

CompTIA (2016) *Quick start guide to security compliance: Cybersecurity: CompTIA, CompTIA.org*. Available at: <https://www.comptia.org/content/guides/quick-start-guide-to-security-compliance#:~:text=The%20first%20step%20is%20start,correct%20secure%20for%20the%20requirement>. (Accessed: 27 January 2024).

European Commission (2024) *What is personal data?, European Commission*. Available at: [https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data\\_en#:~:text=considered%20personal%20data-,Answer,person%2C%20also%20constitute%20personal%20data](https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en#:~:text=considered%20personal%20data-,Answer,person%2C%20also%20constitute%20personal%20data). (Accessed: 27 January 2024).

Information Commissioners Office (2024) *Guide to Law Enforcement Processing, ICO*. Available at: <https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/principles/> (Accessed: 27 January 2024).

Intersoft Consulting (2023) *Art. 6 GDPR – lawfulness of processing, General Data Protection Regulation (GDPR)*. Available at: <https://gdpr-info.eu/art-6-gdpr/#:~:text=processing%20is%20necessary%20for%20the%20purposes%20of%20the%20legitimate%20interests,the%20data%20subject%20is%20a> (Accessed: 27 January 2024).

## Peer response #1



Initial Post

by Nelson Okolie - Sunday, 18 February 2024, 8:55 PM

The need for data protection rules have become very necessary to guarantee the fundamental right to the protection of personal data. This is because of the increase in the value placed on data protection and security by individuals and for businesses to maintain the trust of its clients and act in the right way. In the European Union, the general data protection regulation (GDPR) is a regulation on data protection and privacy while in my home country, the Nigeria data protection regulation (NDPR) is the main data protection regulation in Nigeria. The Nigeria data protection regulation (NDPR) aims to inform Nigerians on how their personal are collected, used, stored, made available, disclosed, updated, safeguarded, destroyed and processed.

In the Nigerian financial sector, there is a growing number of interactions, observations, and regulations the banking enterprises manage through various data acquisition points. Some of the greatest challenges include the hindrance of legacy systems on business performance, the duplication of effort and the high cost in managing multiple systems with manual data entry. Other challenges include the management of compliance with growing data privacy and security concerns. The increase in data volume leading to data governance.

This is where master data management (MDM) becomes useful - the process of creating and maintaining a single master record for each person, place, and thing in a business. The master data management (MDM) tools bring together information across different applications so that it can be managed, leveraged, and integrated across the enterprise, without the burden and expense of managing multiple and isolated systems. Through master data management (MDM), my organization has gained a trusted and current view of key data across its business for better reporting and decision-making.

In my organization, some of the best practices when planning our master data management (MDM) use cases and implementation varies from defining the context and scope, to establishing master data management project leaders and outcomes. Others include ensuring master data management data quality requirements, addressing compliance head on, setting clear goals for data governance, increasing operational efficiency and research deployment options for master data management.

References:

Eur-lex (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at: [Regulation - 2016/679 - EN - gdpr - EUR-Lex \(europa.eu\)](#) (Accessed 26 January 2024).

Semarchy (2022) Seven best practices for master data management in banking. Available at: [Master Data Management in Banking: 7 Best Practices - Semarchy](#) (Accessed 30 January 2024).



Peer Response

by Sahr Solar Sumana - Monday, 19 February 2024, 11:42 AM

The initial post for this topic briefly compared the European GDPR to the compliance law in the country of Nigeria, known as the Nigerian data protection regulation (NDPR). Similarities are shared between the two such as how they guide users of data on how data should be treated once acquired. One example of a similarity is the consent rule NDPR (2019) enforce that "consent may be made through a written statement, sign or an affirmative action signifying agreement to the processing of personal data". Similarly the UK GDPR states that "consent requires a positive opt in, requires a clear statement of consent and must meet the UK GDPR standard" (ICO, no date).

The initial post also provides somewhat of a solution to securing the personal data rule by suggesting the method of Master Data Management (MDM), although this can provide reliability and validity on the acquired dataset it can still make you susceptible to breaches without the correct procedures in line. Returning to the point of consent, for the NDPR, "while oral consent appears valid under the Act, it should be noted that the Act emphasizes that the burden of proof lies with the Data Controller. Hence, the approach and mechanism of obtaining and documenting oral consent should be carefully considered (Anyanwu & Agbaje, 2023).

On the other hand the UK GDPR implies that the "burden of proof" also lies with any third party controllers that rely on the consent from the individual. This shared responsibility could be beneficial as it provides a fail-safe considering proof will be held by more than just one party. However, this could make it harder for individuals to withdraw their consent as they may have to reach out to the third party controllers too.

Reference List:

Anyanwu, J. and Agbaje, O. (2023) *Nigeria Data Protection Act 2023 review*. Available at: [https://assets.kpmg.com/content/dam/kpmg/ng/pdf/nigeria-data-protection-act2023\\_kpmg-review.pdf](https://assets.kpmg.com/content/dam/kpmg/ng/pdf/nigeria-data-protection-act2023_kpmg-review.pdf) (Accessed: 19 February 2024).

ICO (no date) *ICO - Consent, ICO*. Available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/consent/> (Accessed: 19 February 2024).

NDPR (2019) *Nigeria Data Protection Regulation 2019, NIGERIA DATA PROTECTION REGULATION 2019: IMPLEMENTATION FRAMEWORK*. Available at: <https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf> (Accessed: 19 February 2024).

Peer Response #2

by Courtney Sommerville - Monday, 19 February 2024, 1:10 PM

Since GDPR replaced the original data protection directive in May 2018 in the UK it has become the new framework of data protection laws. (Local Government Association) It is set out to ensure personal data is processed securely. It is to ensure confidentiality and to ensure the data is held with integrity.

ICO is the independent supervisory body relating to the UK's data protection legislation. ICO do not regulate any European activities by the EU GDPR.

GDPR sets out 7 key principles in which relate to the processing of personal data. These include:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

These principles are important as they ensure good data protection practice. Not following these rules can leave a company with substantial fines. (ICO,2024). These principles all relate to how data is kept secure. When data is kept only for its sole purpose this is similar to data minimisation because there is not an overload of data, only the data needed for the purpose it is being used for is needed to be stored. However their is a storage limitation so this also relates to data minimisation so if data is kept to a minimum it isn't going to overload the storage space. However accuracy is to ensure the data being kept is accurate and no ones personal data is incorrect. Data needs to be kept with fairness, transparency but also integrity and confidentiality, this ensures personal data is kept safe but is also reliable and fair to the individual whose data it is.

These principles considers risk analysis, organisational policies, and can include physical and technical measures.

References:

ICO. (N.D) A guide to the data protection principles. Available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/> [Date Accessed 17th February 2024].

Local Government Association. (N.D) general data protection regulation (GDPR). Available at: [https://www.local.gov.uk/our-support/research-and-data/data-and-transparency/general-data-protection-regulation-gdpr#:~:text=The GDPR is Europe's new,started on 25 May 2018.](https://www.local.gov.uk/our-support/research-and-data/data-and-transparency/general-data-protection-regulation-gdpr#:~:text=The%20GDPR%20is%20Europe's%20new,started%20on%2025%20May%202018.) [Date Accessed 17th February 2024].

ICO. (N.D) Overview - Data protection and the EU. Available at: [https://ico.org.uk/for-organisations/data-protection-and-the-eu/overview-data-protection-and-the-eu/#:~:text=The ICO remains the independent,close with European supervisory authorities.](https://ico.org.uk/for-organisations/data-protection-and-the-eu/overview-data-protection-and-the-eu/#:~:text=The%20ICO%20remains%20the%20independent,close%20with%20European%20supervisory%20authorities.) [Date Accessed 17th February 2024].

ICO. (N.D) Principle (f): Integrity and confidentiality (security). Available at: [https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/integrity-and-confidentiality-security/#:~:text=You must ensure that you,know as the security principle.](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/integrity-and-confidentiality-security/#:~:text=You%20must%20ensure%20that%20you,know%20as%20the%20security%20principle.) [Date Accessed 17th February 2024].



Peer Response

by Sahr Solar Sumana - Monday, 19 February 2024, 4:08 PM

The initial post outlined the 7 key principles that relate to the personal processing of personal data and further expanded upon these key principles too. Although these 7 key principles can be seen as just as important of each other, it could be argued that lawfulness, fairness and transparency is one of the main building blocks behind the compliance laws set out by GDPR and the ICO.

Consent is the sub-topic behind this principle and both the ICO and GDPR affirm that "processing personal data is generally prohibited, unless it is expressly allowed by law, or the data subject has consented to the processing" (Intersoft, 2021). Under interpretation this principle suggests that without consent organisations would be able to source personal data without the consent of the individual which is not just unethical but also promotes a lack of security.

Data minimisation is also another highlighted principle, I agree that it does lead to less storage space being occupied which is beneficial. However ICO added another layer to this principle suggesting that data minimisation restricted organisations to only collecting and storing "adequate and relevant data that is limited to what is necessary for the intended purpose" (ICO, no date). For example "a debt collection agency that's trying to locate a particular debtor. After processing information on several people with a similar name, it finds the right person. At this point, the agency must delete the relevant records for the people whose information it collected during its search" (Irwin, 2023). Not deleting this data could leave more parties susceptible to a risk if there is a data breach.

Reference List:

ICO (no date) *Principle (c): Data minimisation*, ICO. Available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/the-principles/data-minimisation/> (Accessed: 19 February 2024).

Intersoft (2021) *Consent, General Data Protection Regulation (GDPR)*. Available at: <https://gdpr-info.eu/issues/consent/> (Accessed: 19 February 2024).

Irwin, L. (2023) *What is Data Minimisation? definition & examples*, IT Governance UK Blog. Available at: <https://www.itgovernance.co.uk/blog/what-is-data-minimisation-definition-examples> (Accessed: 19 February 2024).