BANWO & IGHODALO

OPENNESS OR TRANSPARENCY IN DATA PROCESSING

27/05/2021

One of the side effects of the digital revolution has been the vast increase in the volume of digital data now being generated, characterized by the four "Vs"- volume, velocity, veracity and variety. Smart appliances have significantly changed the way that we interact with the world, and with one another, and this is becoming increasingly governed by data. Through our smartphones we, have become human data factories, generating vast amount of information daily. Further, new sources of information, like the social media, call detail records, sensors, 5G enabled devices, tracking applications, and satellite imagery provide the opportunity to produce even more data. With increasing reports of data breaches and misuse of data, people are understandably wary about trusting companies with their personal information. Accordingly, increasing attention is being paid to data protection and privacy issues. Various countries are coming up with legislations prescribing standards for proper handling of data, particularly, personal data.

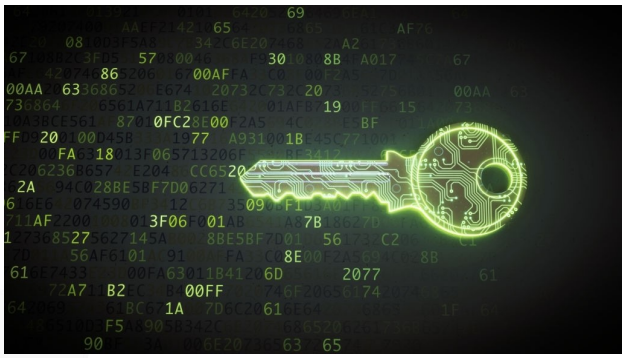
One of the safeguards provided by data protection regulations is the requirement that, any information and communication concerning the processing of personal data must be easily accessible and easy to understand. Such information is required to be presented in clear and plain language. this requirement is often described as the principle of transparency or openness of data processing. Article 5(1) of the European Union's General Data Protection Regulation (**"GDPR"**) stipulates, in this regard, that *"personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')".*

The ***OECD Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data*** provides in Article 12 that, *there should be a general policy of openness about developments, practices and policies with respect to personal data. Mechanisms should be readily available* of *establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller*. Article 2.5 of the Nigeria Data Protection Regulation 2019 (**"NDPR"**) stipulates that, *notwithstanding*

OPENNESS OR TRANSPARENCY IN DATA PROCESSING

anything contrary in this Regulation or any instrument for the time being in force, any medium through which Personal Data is being collected or processed shall display a simple and conspicuous privacy policy that the class of Data Subject being targeted can understand.

The implication of the foregoing is that, any information addressed to the public or to the data subject must be concise, easily accessible and easy to understand. Clear and plain language including, where appropriate, visualisation should be used.



In a recent decision by the National Data Protection Commission (CNIL), leading to the imposition of a €50million fine on GOOGLE, the decision was based on findings that the information provided by GOOGLE was not easily accessible for users. Essential information, such as the data processing purposes, the data storage periods or the categories of personal data used for GOOGLE's adverts personalization, were excessively disseminated across several documents, with buttons and links on which users are required to click to access complementary information. The relevant information was accessible after several steps only, implying sometimes up to 5 or 6 actions. It was also observed that some information wasn't always clear nor comprehensive and as a result, users were not able to fully understand the extent of the processing operations carried out by GOOGLE. Further, the purposes of processing and the categories of data processed for these various purposes, were described in a manner that was too generic and vague and that the information about the retention period was not provided for some data.

Information about data processing is usually provided in data protection policy documents, such as privacy policies, privacy notices, and consent clauses. Compliance with transparency requirement is not achieved merely by preparing and publicizing data protection policy documents. Information provided in these documents must be clear and comprehensive to enable data subjects fully understand the extent of the processing operations to be carried out. In addition to the manner of presentation, the nature of information provided in data protection policies must be comprehensive. In this regard, Article 2.5 of the NDPR states that *"The privacy policy shall in addition to any other relevant information contain the following:*

a. *What constitutes the Data Subject's consent;*
b. *Description of collectable personal information;*
c. *Purpose of collection of Personal Data;*
d. *Technical methods used to collect and store personal information, cookies, JWT, web tokens etc.;*
e. *Access (if any) of third parties to Personal Data and purpose of access;*
f. *A highlight of the principles stated in Part 2;*

OPENNESS OR TRANSPARENCY IN DATA PROCESSING

g. *Available remedies in the event of violation of the privacy policy; and*

h. *The time frame for remedy."*

The foregoing is clearly the minimum requirement and data controllers should ensure that, as much information as may be necessary to enable data subjects fully understand the extent of the processing operations to be carried out, is provided in their data protection policy documents. Such additional information may include the identity and contact details of the controller and Data Protection Officer as required by Article 13 of the GDPR. Naturally, the extent and type of information required to meet this requirement will vary depending on the nature and complexity of the processing operation, provided in any case that the minimum requirement as provided in the NDPR is complied with.

In addition, careful consideration should be given to the manner in which the information is presented and the class of data subject being targeted in the preparation of data protection policy documents. Information must be presented in a manner that is easily comprehended by the class of data subject being targeted. Obviously data information directed at professionals will be presented differently from information aimed at the public at large or at children.

Failure to meet this requirement may have far reaching consequences, including, as in the GOOGLE case, invalidating or making consent inadequate. Both the NDPR and the GDPR require consent to be a voluntary and informed decision. Where data subjects do not have enough information about the nature and extent of the processing operations, it is doubtful if consent provided in such circumstances can be informed or voluntary, as the data subject does not have enough information about the processing operations to ascertain its impact on his rights and freedom and therefore give his consent from an informed position.

Transparency in data management processes engenders trust by data subjects in dealing with a data controller. In the current digital age, where interaction with providers of goods and services results in processing of data, good data management processes play a key role in winning and retaining customers and their trust. Building customer trust in this digital age now extends to the way an organisation manages personal data. The journey to building customer trust requires organisations to establish a strong foundation and adequate data management processes, with transparency as its cornerstone.

OPENNESS OR TRANSPARENCY IN DATA PROCESSING

The Grey Matter Concept is an initiative of the law firm, Banwo & Ighodalo.

DISCLAIMER: This article is only intended to provide general information on the subject matter and does not by itself create a client/attorney relationship between readers and our Law Firm or serve as legal advice. We are available to provide specialist legal advice on the readers' specific circumstances when they arise.

Further enquiries should be directed to the Contact Persons above or to the **Intellectual Property & Technology Practice Group** at ipgroup@banwo-ighodalo.com

Olumide Osundolire
Partner
E: oosundolire@banwo-ighodalo.com

Thelma Okorie
Associate
E: TAbu@banwo-ighodalo.com

Rouna Erhieyovwe
Associate
E: rerhieyovwe@banwo-ighodalo.com