NICCOM LLP
BARRISTERS & SOLICITORS

**Privacy and Data Protection Snapshot Series**

**Processing of personal data – Meaning of, and legal bases for**


***What is processing?***

The word "processing" is perhaps the most common word one comes across in any discourse relating to privacy and data protection compliance.

Processing refers to any and every action taken by a data controller or data administrator in relation to the personal data of one or more data subjects. It covers the collection of personal data to destruction of such data, and all actions in-between. The Nigeria Data Protection Regulation 2019 ("NDPR") defines processing to mean *"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."*

Many everyday actions – the collection of an employee's biodata information using an employee onboarding form, the storage of a company's Vendor Masterfile (containing personal data) remotely, the update of an individual customer's residential address, the destruction of paper files containing personal information of deceased employees, sending sales information containing personal information to a parent company outside Nigeria – would qualify as "processing" under the NDPR and the GDPR. It is immaterial whether such actions were performed using computer systems or other automated means or not.

***Legal basis for processing personal data***

A data controller must have a recognisable ground to lawfully process the personal data of one or more data subjects. The NDPR recognises five legitimate bases for processing personal data, and they are as follows:

1. Consent. A data controller may process personal data of a data subject where such data subject has given consent to the processing of the data for one or more specific purposes. For instance, when visiting some websites or accessing some apps, it is common to see pop-ups requiring the consent of users before certain information can be accessed by such users. Some companies also require users to elect as to whether their information will be stored by such companies. All these instances are scenarios where consent is sought by data controllers.

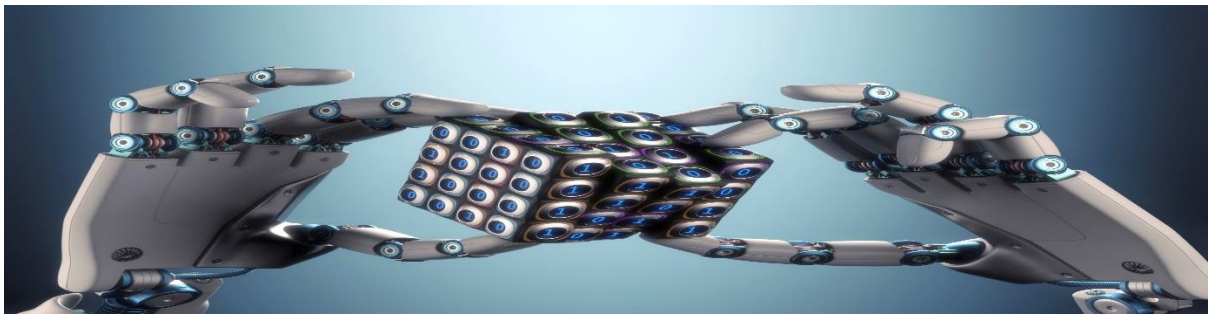
   It is important to point out that consent must be clear and positive – that is, by means of a positive action. Negative or implied consent is not recognised under the NDPR (or the General Data Protection Regulation ("GDPR"), for that matter).

2. Performance of contract. A data controller may process personal data where such processing is necessary for the performance of a contract to which the data subject is a party to. Where the terms of a contract between parties expressly or impliedly permits one party to process the personal data of the other party, it is lawful to process such data.

   For instance, the nature of tenancy agreements, employment contracts envisage that the personal information of the affected tenant or employee will be processed by the landlord/employer. Again, one can reasonably infer that the filling out of an account opening form would empower the bank to process one's information, at least for account opening purposes.

3. Legal obligation. There are instances where a data controller is obliged to perform certain actions on personal data maintained by it due to a legal or regulatory requirement. For instance, a bank is required to store details of transactions (which may include personal details of a data subject) for a certain period, under the anti-money laundering regulations issued by the Central Bank of Nigeria. Again, a data controller may lawfully transmit personal information of a data subject on the order of a court or at the request of a duly authorised regulator.

4. Vital interest. A data controller may process personal data where such processing is necessary to protect the vital interests of the data subject or of another natural person. The personal data of an unconscious accident victim may lawfully be collected or otherwise processed by a medical facility, for the purpose of rendering lifesaving services to him or her.



5. Public interest. A data controller may also process personal data necessary for the performance of a task carried out in the interest of the public or in exercise of official public mandate vested in the data controller (or administrator). Thus, government agencies may process personal data necessary for official work, in line with establishing laws. Private companies engaged by the government are similarly empowered, where such processing is reasonably inferable from the terms of engagement.

   *** A sixth basis, legitimate interest, exists. This basis is recognised under the GDPR, but was not expressly listed in the NDPR. It relates to processing activities that is reasonably expected to be undertaken by a data controller, for instance the use of such data for forensic audit or marketing purposes. However, for legitimate interest to qualify as a legal basis for processing personal data, the data controller must consider two questions (otherwise known as the *balancing test*). One, is this processing activity necessary for the data controller to function? Two, does the processing activity outweigh any risks to a data subject's rights? If any of the questions can be answered in the negative in any instance, the data controller **cannot** rely on legitimate interest as its legal basis for processing personal data in that instance.

No one legal basis is superior to the other – the use of each depends on the nature of processing intended. A data controller must determine the appropriate legal basis for processing the personal data of a data subject (or a class of data subjects) prior to such processing. Any legal basis relied on by a data controller must also be always demonstrable.

Finally, sensitive personal information (such as race, ethnic origin, religion, trade union membership, sexual orientation, and health data) have unique legal bases for processing, including preventive or occupational medicine, public health, collective bargaining agreements, legitimate activities of not-for-profit organisations, etc.

**NICCOM LLP is a licensed Data Protection Compliance Organisation (DPCO), and can provide data protection compliance audit services, as well as other related services required by businesses. As a law firm, we are positioned to proffer legal advice on the impact of the NDPR to your organisation, and suggest recommendations on process improvement, where necessary**