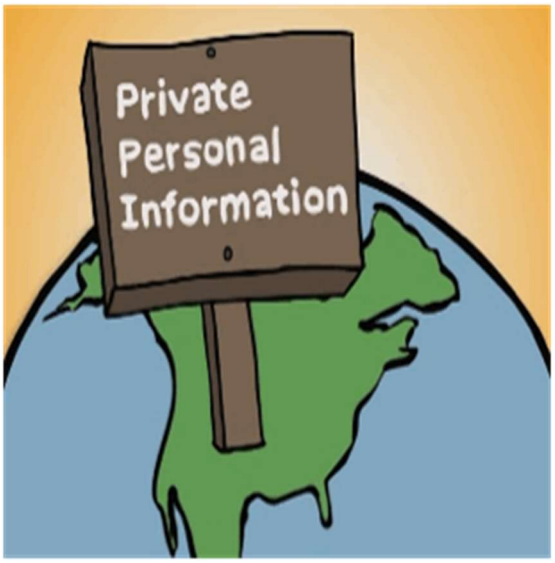
NICCOM LLP
BARRISTERS & SOLICITORS

Privacy and Data Protection Snapshot Series

Personal data



What is personal data

Personal data, or personal identifiable information, refers to data that can be used to identify a person. The EU General Data Protection Regulation (GDPR) defined personal data as "any information relating to an identified or identifiable individual", and went on to define an identifiable person as "one who can be identified, directly or indirectly, in particular by reference to an identification number (e.g., social security number) or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity…"

Personal data includes direct and specific information such as names, phone numbers, IP addresses, national ID numbers, personal email addresses, banking and other financial information, date of birth, family background, place of birth, social media accounts, and so on. It also includes descriptions which can be used in conjunction with other information, to identify a person. For instance, the description "that fair man that dropped his daughter off in a Silver 2015 RAV4 with vehicle plate number ABC-123-DEF…" would qualify as personal data, as it sufficiently discloses the identity of the data subject to the target audience.

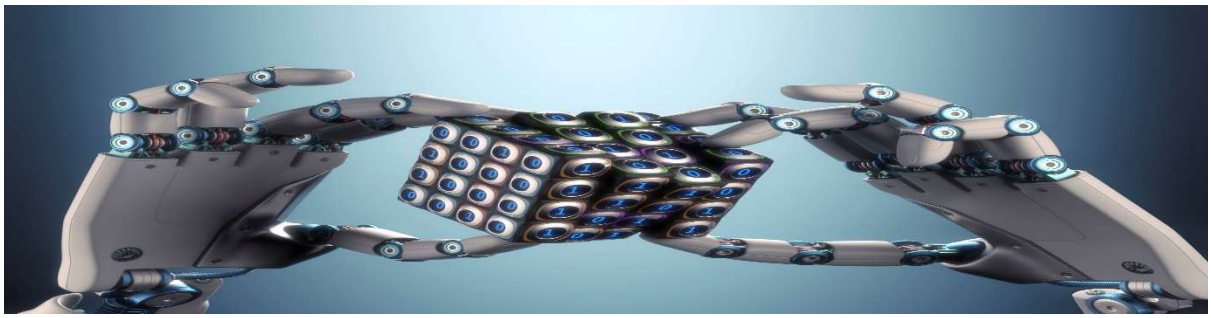
Sensitive personal data is a sub-category of personal data. It refers to a specific set of 'special personal data' that must be treated with extra security. Sensitive personal data includes genetic data (e.g., DNA information), biometric information (e.g., fingerprint data), health information and/or records, religious beliefs, sexual orientation, political views, racial or ethnic origin, trade union membership, criminal records, etc. Data controllers processing sensitive personal data must, in addition to having a legal basis for so doing (refer to the third instalment of our snapshot series for a discussion on the legal bases for processing personal data), ensure that such data is stored securely, using encryption and pseudonymisation techniques.

What "personal data" is not

We have underscored the point that data protection is strictly concerned with the protection of data relating to natural persons (i.e., human beings) in earlier instalments of this series. No other category of legal persons is covered under data protection. Thus, information relating to a company, business, association, or agency (as against the individuals that make up the company, business, association, or agency) will not qualify as personal data. Excluded data will include company registration number,

company address, company tax ID, business address, non-personal email address such as info@dataprotection.com, marketing strategy, or trade secrets.[1]

Not every information relating to a natural person would qualify as personal data. Data that has been anonymised such that the subject is not identifiable can no longer be considered personal data. However, for personal data to be truly anonymised, such anonymisation must be irreversible.



Ownership vs. use of personal data – An aperçu

Personal data are generally owned[2] by the concerned data subjects. In most cases, the data subject is free to use the data in any manner, and to authorise the use of such data by others either absolutely or with restrictions.

Some categories of personal data are not so owned by the concerned data subjects. A mobile number or a bank account number is technically 'owned' by the issuing controller – such numbers can, under certain circumstances, be reissued to another subscriber by the controller. An international passport remains the property of the issuing country, and thus the passport ID number, while identifying a particular data subject, cannot be said to be 'owned' by that data subject.

Conversely, a data subject may belong to a data subject, but possessory rights over such data may be exercised by another person or authority. Fingerprints collected during criminal profiling would fall under this category – while the fingerprints belong to a specified data subject, it is kept in the database of the Police of other investigative authority.

So, can a data subject have any data privacy rights in relation to data not 'owned' or 'possessed' by that subject?

It is submitted that the enjoyment of data privacy rights is not solely dependent on legal ownership or possession. Privacy rights in relation to personal data enures to the relevant data subject automatically, whether or not such information is owned by it. A data controller cannot hide under

[1] Work-related information relating to a specific individual may still qualify as personal data. For instance, while info@dataprotection.com may not qualify as personal data, john.doe@dataprotection.com would qualify as such, as it identifies a specific human being.

[2] Ownership here connotes the ability to exercise absolute possessory rights over such data and exclude others from using the data.

the umbrella of perceived ownership or possession to use the personal data of its data subjects in non-compliance with the NDPR and other extant laws and regulations.

Every data controller must ensure that its use of personal data is clearly justifiable under one or more legal bases, which basis (or bases) must be documented. In addition, any change to personal data, as well as the reason for such change, must be communicated to the affected data subjects. Where the consent of the data subject is required for such change, consent must be clear and positive.

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.