Key Definitions

* **Data Subject**

Data subject refers to any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity.

* **Data Protection Officer**

The primary role of the data protection officer (DPO) is to ensure that the organisation processes the personal data of its members any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.

Under data protection and privacy legislation, data subjects have a number of rights in relation to their personal data. These rights include:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure (“the right to be forgotten”)
5. The right to data portability
6. The right to object to processing (for certain purposes)
7. The right to restriction
8. Rights in relation to automated decision-making, including profiling
9. The right to be informed

Where personal data is being gathered, the data subject must be informed of the following information:

* The identity and contact details of the data controller e.g. the company collecting the information
* The contact details for the Data Protection Officer (“DPO”) of the company
* The reason for collecting and processing the personal data including the lawful basis
* Who the data may be shared with e.g. any third-party processors
* Where applicable, if the personal data will be transferred outside of the European Economic Area (EEA) and details of the safeguards in place for such transfers
* The retention period or the criteria used to define the retention period for the personal data
* The existence of the following rights for data subjects: access, rectification, erasure, portability, object (including the withdrawal of consent where relying on this as a lawful basis), restriction and rights in relation to automated decision-making including profiling, and how to exercise these rights in relation to the personal data held
* The right to lodge a complaint with the relevant DPSA
* Where the provision of the personal data is a statutory or contractual necessity and what the possible consequences are in the absence of providing the personal data

The above information must be provided to a data subject when first obtaining their personal data. One common approach of providing such information, (but not limited to), is in the form of a Data Privacy Notice ("DPN", also known as a Privacy Notice).

1. The right of access

The right of access is also referred to as a Data Subject Access Request (“DSAR”). Data subjects have the right to know what personal data is held in relation to them, the reasons for holding this data, the length of time it is held for, and who the data is disclosed to. DSARs cover any personal data that identifies or relates to an identifiable living individual. There are a number of restrictions outlined within data protection and privacy legislation relating to the extent of a data subject’s right to access their personal data, for instance, personal data relating to other data subjects should not be disclosed unless the appropriate authorisation has been obtained. DSARs may need to be redacted or withheld to protect the privacy rights of other data subjects. You should refer to local processes and procedures on how to action a DSAR when such a request is received by the Group.

When does the clock start?
The clock starts ticking the day the Group receives the request, not the date it is sent to a specific business unit or department. The Group is required to fulfil the request within one calendar month.

Example
A request is received on 03.09.2019. Start fulfilling the request upon receipt and the verification process can take place in parallel to help speed things along. Before a response is issued, ensure it is a genuine request and verify the person making the request is legally entitled to the information. Fulfil in advance of 03.10.2019.

1. The right to rectification

The right to rectification is the right of a data subject to have their personal data corrected where it is factually inaccurate or incomplete. If inaccurate personal data is used, this can have a number of adverse consequences for both the data subject and the Group. Business units must inform third parties and/or data processors of a change to personal data if applied, and inform the individual about the third parties we have disclosed their personal data to, where appropriate.

You should refer to your business unit processes and procedures on how to action a request of rectification when it is received by the Group. Please note that requests to update personal data in the course of everyday business are not rectification requests e.g. change of address should be managed in line with your business unit procedures.

1. The right to erasure (“the right to be forgotten”)

The right to erasure is often referred to as ‘the right to be forgotten’. Data subjects have the right to request their personal data be erased where there are no compelling bases for the personal data to be held any longer, for example, if the personal data is no longer required for the purpose it was first collected or where the processing is based on consent and that consent is withdrawn or it has to be erased in order to comply with a legal obligation.

1. The right to data portability

The right to data portability applies in certain circumstances and enables data subjects to obtain specific elements of their personal data and/or have request that their personal data is transmitted to another data controller. This means being able to transmit the personal data in a format that can be reused and is machine-readable, meaning a file format structured so that software applications can easily identify, recognise and extract specific data

1. The right to object to processing (for certain purposes)

The right to object provides data subjects with a right to object to the processing of their personal data in certain circumstances such as where there is no lawful basis for processing the personal data, or consent-based direct marketing. The Group must stop processing the personal data unless it can demonstrate a compelling lawful basis for the processing activity to continue.

1. The right to restriction

The right to restriction gives data subjects the right to request that their personal data is restricted from processing. Where such a request is made, the data can be held, but it must not be subject to any further use. Examples where restrictions apply include:

* Where a data subject believes that the personal data is inaccurate, its use must be restricted until the accuracy has been verified
* Where a data subject objects to the processing of their personal data, its use must be restricted while investigating if there is a compelling reason as to why the processing is required

As with all data subject rights, if any personal data is processed by a third party or data processor, they must also comply with this right as instructed by the Group.

1. Rights in relation to automated decision-making, including profiling

Data protection and privacy legislation provides safeguards for individuals against the risk that a potentially-damaging decision is taken without human intervention. All data subjects have the right not to be subject to a decision when it:

* Is based on automated processing
* Produces a legal effect or a similarly significant effect on the individual

In order to comply with a data subject's rights regarding automated decision-making and profiling, the Group must ensure that data subjects are able to:

* Obtain human intervention in relation to decision-making
* Express their point of view
* Obtain an explanation of the decision and the ability to challenge it

Restrictions:

There may be circumstances when the Group may not be obliged to fulfil a data subject request in relation to their privacy rights. There are also certain limitations contained within the data protection rights as set out in legislation, such as:

* A data subject’s right to obtain a copy of their personal information under the rights of access or portability should not adversely affect the privacy rights of others e.g. personal data relating to others should not be disclosed, unless the appropriate permission has been obtained
* Certain data protection rights only apply in specific circumstances, for example, the right to erasure, more commonly known as ‘the right to be forgotten’, only applies under certain conditions, such as where the personal data is no longer required for the purpose it was originally collected
* In certain very limited circumstances, organisations may charge a fee for responding to a request, or even to refuse to act on a request, if the request is unfounded or excessive

Some additional restrictions are as follows:

* The exercise or defence of legal claims
* Personal data relating to an opinion given in confidence