DATA PROTECTION OFFICER

Subject to the General Data Protection Regulation ((EU) 2016/679) (GDPR), the Directors have agreed to appointed one of Company's employees as a Data Protection Officer on the terms set out herein and in a contract of employment entered into in any particular case.

The Data Protection Officer (DPO) shall monitor internal compliance with all relevant privacy-related legislation, inform and advise on Company's data protection obligations, provide advice regarding Data Protection Impact Assessment (DPIA) and act as a contact point for data subjects and the supervisory authority.

Role and Responsibilities

In his/her role, the DPO shall primarily be responsible for:

- implementing measures and a privacy governance framework to manage data use in compliance with the GDPR, including developing templates for data collection, assisting with data mapping, and customer, counterparty, vendor and other third parties management reviews;
- working with key internal stakeholders in the review of projects and related data to ensure compliance with local data privacy laws, and where necessary, complete and advise on privacy impact assessments;
- serving as the primary point of contact and liaison for the Commissioner for Personal Data Protection and other EEA Data Protection Authorities on all data protection related matters under the GDPR;
- serving as the primary point of contact for data privacy laws related queries within the Company;
- monitoring changes to local privacy laws and making recommendations to the relevant departments of the Company;
- setting standards and reviewing policies and procedures globally that meet the requirements under the GDPR and any localization requirements in countries of operation;
- developing and delivering privacy training to various functions in the Company;
- developing strategies and initiatives to ensure engagement with key internal and external stakeholders;
- coordinating and conducting data privacy audits;
- collaborating with information security function to raise employee awareness of data privacy and security issues;
- collaborating with information security function to maintain records of all data assets and exports, and maintaining a data security incident management plan to ensure timely

remediation of incidents including impact assessments, security breach response, complaints, claims or notifications, and responding to subject access requests (SARs);

- ensuring that Company's services, products, activities, systems and procedures comply with all relevant data privacy and protection law, regulation and policy (including in relation to the retention and destruction of data);
- promoting effective work practices, working as a team member, and showing respect for co-workers;
- working with designated privacy law attorneys across the Group and, where necessary, outside counsel to help advise on local data privacy law issues.

Compliance Program

As part of the managing data protection compliance programme, the DPO shall:

- inform and advise the Company of its legal obligations regarding data protection;
- participate in meetings where decisions with data protection implications are taken;
- update procedures and internal guidance where necessary relating to the processing of personal information;
- maintain a register documenting all personal information processing activities within the Company;
- define and maintain information flow maps within the Company, and between the Company and its customers, counterparties, vendors and other third parties;
- maintain a log of any data protection incidents and remedial recommendations and actions;
- ensure that DPIAs are performed when appropriate;
- advise those performing DPIAs as necessary;
- respond to individuals whose data is processed on all issues related to the processing of their data and the exercise of their rights;
- offer consultation on how to deal with privacy breaches.

Monitoring

As part of the monitoring data protection compliance programme, the DPO shall:

- highlight and develop solutions for any issues relating to the fair obtaining, use and storage of personal data, information quality and integrity, technical and organizational security;
- participate in a legitimate interests assessment (LIA). The Company will seek input and advice of the DPO, on the following issues, amongst others:
    (i) whether or not to carry out a LIA;

(ii) identifying the legitimate interest(s);

(iii) applying the necessity test;

(iv) doing a balancing test;

(v) keeping a record of a LIA and its outcome;

(vi) keeping a LIA under review and refreshing it if there is a significant change in the purpose, nature or context of the processing;

(vii) if a LIA identifies significant risks, whether the Company needs to do a DPIA to assess the risk and potential mitigation in more detail;

(viii) how to tell people in Company's privacy information that the Company is relying on legitimate interests, and to explain what these interests are.

- participate in a DPIA. The Company will seek the advice of the DPO, on the following issues, amongst others:

(i) whether or not to carry out a DPIA;

(ii) what methodology to follow when carrying out a DPIA;

(iii) whether to carry out the DPIA in-house or whether to outsource it;

(iv) what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects;

(v) whether or not the DPIA has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR;

(vi) if the Company disagrees with the advice provided by the DPO, how the DPIA documentation should justify why the advice has not been taken into account.

(a) provide annual reports to the Board on the Company's data protection compliance, training and awareness.

Training

As part of the training and awareness programme, the DPO shall:

- provide advice and training to staff and managers to raise awareness and understanding about their responsibilities regarding data protection and other associated legislation or good practice;
- liaise with the Commissioner for Personal Data Protection to develop and implement a data protection awareness and training programme;
- maintain and update own knowledge of developments in data protection issues, information management and related legislation;
- ensure written information on data protection is available for provision to customers, counterparties, vendors and employees, including appropriate privacy notices;

- provide a consultancy service for all departments, including liaison, assessing problems, queries, procedures and practices and take responsibility for advice given;
- continue to keep abreast of developments in the field of data protection by attending appropriate conferences and continuing personal development, as necessary.

Reporting

The DPO shall report directly to the Board on all matters within the DPO's duties and responsibilities and on how the DPO has discharged his/her responsibilities and shall maintain open communication with the Chairman.

The DPO shall annually produce to the Board a formal report of his/her activities setting out the Company's strategy and policies in relation to data protection. The report shall describe the work of the DPO, including:

(a) a summary of the role of the DPO in relation to data protection, including data protection risks to which the Company may be exposed and how they arise, the Company's objectives, policies and processes for managing risks;

(b) methods used to measure the risks, and changes from the previous reporting period;

(c) the scope and outcome of the data protection programmes;

(d) a report on the way the DPO has discharged his/her responsibilities; and

(e) whether external advice was taken.

Authority

The Company shall not give the DPO instruction on how to carry out his/her tasks. Thus, the DPO will not be instructed how to deal with a matter, such as how to investigate a complaint or what result should be achieved.

Where the Company decides to take a certain course of action despite the DPO's advice to the contrary, the DPO will be given the opportunity to make his/her dissenting opinion clear to the Board and to any other decision makers.

The DPO is allowed to have other functions provided that these do not give rise to conflicts of interests. This entails in particular that the DPO cannot hold a position within the Company that leads him / her to determine the purposes and the means of the processing of personal data.

The DPO shall be bound by secrecy and confidentiality in the performance of his/her tasks.

The Company shall provide adequate support of the DPO in terms of financial resources, infrastructure (premises, facilities, equipment) and staff where appropriate.

The Company shall provide the DPO with necessary access to other services, such as Legal, IT, etc., so that the DPO can receive essential support, input and information from those other services.

The Company shall give the DPO the opportunity to stay up to date with regard to developments within data protection; the DPO will be encouraged to participate in training courses on data protection and other forms of professional development, such as participation in privacy fora, workshops, etc.

The Company will publish contact details of the DPO and communicate the contact details of the DPO to all relevant supervisory authorities.