PERSONAL DATA PROTECTION POLICY

1. Introduction

The Scomi group of companies, which comprise Scomi Group Bhd and its subsidiaries, ("the Group") need to keep certain personal data, for example about its current, past and prospective employees, customers, suppliers and directors, to fulfil its purpose and to meet its legal obligations to these parties and the government. To comply with the laws relating to the protection of personal data, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the Group must comply with the data protection principles which are set out in the relevant laws governing the protection of personal data in each of the countries in which it operates.

In order to ensure that this happens, the Group has developed and adopted this Personal Data Protection Policy. This policy sets out Group's rules on data protection and the conditions that must be satisfied in relation to the collecting, obtaining, handling, processing, storage, transportation and destruction of personal and sensitive information. The Group and all its employees who process or use personal information must ensure that they follow the principles set out in this Policy at all times.

2. Status Of This Policy

This policy has been approved by the Boards of Scomi Group Bhd, Scomi Energy Services Bhd and Scomi Engineering Bhd for adoption by their respective groups of companies and any breach will be taken seriously and may result in disciplinary action up to and including dismissal.

Any person who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with their immediate superior or the Group Data Protection Officer in the first instance.

3. Definition Of Data Protection Terms

Data subject for the purpose of this policy refers to any individual about whom the Group holds personal data and includes, its current, past and prospective employees, customers, suppliers and directors.

Data processor means any third party who processes personal data on for or on behalf of any company within the Group.

Personal data means information relating to an individual who can be identified from that information (or from that and other information that is in, or is likely to come into, the possession of the data user). Personal data can be factual (such as a name, address, date of birth, mobile phone number, personal email address or salary details) or it can be an opinion (such as a performance appraisal) and includes images (such as photographs or X-rays) or recordings (whether video or sound).

Processing means performing any operation or set of operations on personal data, including:

- obtaining, recording or keeping personal data,
- collecting, organising, storing, altering or adapting the personal data,
- retrieving, consulting or using the personal data,
- disclosing the information or personal data by transmitting, transfer, disseminating or otherwise making it available,
- aligning, combining, correcting, erasing or destroying the personal data.

Sensitive personal data includes information about a person's racial or ethnic origin, gender, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, criminal convictions or the alleged commission of an offence. Sensitive personal data can

only be processed under strict conditions, and will usually require the express consent of the person concerned.

4. Data Protection Principles

Anyone processing personal data must comply with the following principles of good practice. These provide:

a. That personal data shall be obtained and processed fairly and for a lawful purpose directly related to an activity of the Group, with the consent of the data subject, and shall not be processed unless it is:
    - necessary for or directed related to that purpose; and
    - adequate, relevant but not excessive in relation to that purpose.

b. That written notice shall be given to the data subject as soon as practicable specifying, amongst others:
    - a description of the personal data being processed and its purpose,
    - the data subject's right to access and correct the personal data,
    - third parties to whom personal data may be disclosed,
    - of the data subject's choice to limit the processing of personal data,
    - whether supply of personal data by data subject is obligatory or voluntary, and if the former, then the consequences of failure to supply the personal data.

c. That personal data shall be used and disclosed only in ways compatible with these purposes.

d. That personal data shall be kept safe and secure from loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

e. That personal data shall not be kept for longer than is necessary for that purpose.

f. That personal data shall be accurate, complete, not misleading and kept up-to-date.

g. That data subjects shall be provided access to their personal data on request.

5. Notification of Data Held and Processed

All employees and other data subjects are entitled to:

- Ask what information the Group holds about them and why.
- Be informed of the third parties to whom the Group may disclose the personal data.
- Ask how to gain access to it.
- Be informed how to keep it up-to-date.
- Be informed what the Group is doing to comply with its obligations under the applicable laws and regulations governing the protection of personal data.
- Be informed of the consequences for data subjects who fail to supply their personal data.

6. Responsibilities of Data Subjects

All data subjects are responsible for:

- Checking that any personal data that they provide to the Group is accurate and up to date.
- Informing the Group of any changes to information which they have provided, e.g. changes of address.
- Checking any information that the Group may send out from time to time, giving details of information that is being kept and processed.

If, as part of their responsibilities, employees collect information about other people (e.g. about subordinates and other employees), they must comply with this Policy, the Data Protection Guidance Notes and any other guidelines and/or procedures issued by the Group in relation to this policy.

7. Data Security

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All employees are responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

Detailed advice on data security is contained in the Data Protection Guidance Notes.

8. Rights to Access Information

Employees and other data subjects of the Group have the right to access any personal data that is being kept about them on computer and also have access to paper-based data held in certain manual filing systems. Any person who wishes to exercise this right should make the request in writing to the Group Data Protection Officer, using the standard Personal Data Access Request Form. The Group may charge a reasonable fee on each occasion that access is requested.

The Group aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of receipt of a completed form unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

9. Third Party Data Processors

The Group shall ensure that where personal data is processed by a data processor for and on behalf of any company within the Group, such data processor must:

a. guarantee security measures are implemented to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction; and
b. take reasonable steps to ensure compliance with those measures.

10. Personal Data in the Public Domain

Information that is already in the public domain is exempt from this Policy. This would include, for example, information on data subjects contained within externally circulated publications. Any individual who has good reason for wishing details in such publications to remain confidential should contact the Group Data Protection Officer.

11. Data Subject's Consent

The need to process personal data for normal purposes has been communicated to all data subjects. In some cases, if the personal data is sensitive, for example information about health, religious or political beliefs or opinions or record of offences or alleged offences, express consent to process the data must be obtained. Processing may be necessary to operate the Group's policies, such as health and safety.

12. Retention of Personal Data

Personal data should not be kept longer than is necessary for the purpose it was collected. For guidance in relation to particular retention periods for personal data, employees should refer to the Data Protection Guidance Notes and the Personal Data Retention Schedule. The Group has various legal obligations to keep certain employee data for a specified period of time. In addition, the Group may need to retain personnel data for a period of time in order to protect its legitimate interests.

13. Transferring Personal Data Across Borders

As the Group operates internationally and has third party service providers outside of the country where the personal data was originally collected, it may be necessary in the course of business that any company within the Group has to transfer a data subject's personnel data to other countries which do not have comparable data protection laws. This transfer of personal data is necessary for the management and administration of contracts to which a company within the Group is party to or to facilitate human resources administration within the Group. When this is required, the Group will take steps to ensure that the data has the same level of protection as it does in the country where the personal data was originally collected.

14. The Group's Designated Data Controller

Each company within the Group is the data user of personal data collected by that company and is therefore ultimately responsible for implementation of this Policy. However, the Group Data Protection Officer will deal with the day-to-day matters arising from this Policy. Any questions or concerns about the interpretation or operation of this Policy should be taken up in the first instance with the Group Data Protection Officer.

15. Review of this Policy

This Personal Data Protection Policy was adopted by:

- the Board of Directors of Scomi Engineering Bhd on 18 February 2014;
- the Board of Directors of Scomi Energy Services Bhd on 19 February 2014; and
- the Board of Directors of Scomi Group Bhd on 20 February 2014.

Any subsequent amendment to the Personal Data Protection Policy can only be approved by the aforementioned Boards of Directors.

The Personal Data Protection Policy shall be periodically reviewed and may be amended from time to time by the abovementioned Boards as they deem appropriate.

The Personal Data Protection Policy is available on the websites of Scomi Engineering Bhd, Scomi Energy Services and Scomi Group Bhd.