YINSON HOLDINGS BERHAD

Data Privacy

POLICY & PROCEDURE

01	23-Jun-2020	Issue for Approval	Legal Counsel	Head of IT	Board
Rev No.	Date	Reason for Issue	Prepared by	Checked by	Approved by

Document Title:	Data Privacy Policy & Procedure		
Document No:	YHB-LE-CG-PP-0002		
Process:	Document Control	**Applicable To:**	YINSON Group of Companies
Revision No:	01	**Effective Date:**	23 June 2020

Table of Contents

Revision Details

Rev. No.	Section	Details
01		New Policy Adoption

OBJECTIVE:

We view it as our duty, as an international corporation, to comply with the various legal regulations around the world that govern the management of personal data. Our top priority is to ensure universally applicable, worldwide standards for handling personal data.

For us, protecting the personal rights and privacy of each and every data subject is the foundation of trust in our business relationships.

We shall achieve this by:

Our Yinson Corporate Data Privacy Policy ("Data Privacy Policy" or "Policy") lays out strict requirements for processing personal data pertaining to customers, prospects, business partners and employees. We shall strive to meet the requirements and ensure compliance of the various applicable principles of national and international data protection laws in force all over the world. The policy sets a globally applicable data protection and security standard for our company and regulates the sharing of information between our Yinson Group of Companies ("Yinson Group").

Our data privacy officers and employees are obligated to adhere to the Corporate Data Privacy Policy and observe their local data protection laws.

Our Data Privacy Team will be pleased to answer any questions you have about data protection and security at Yinson Group.

This Policy is applicable to all Yinson Group personnel, contractors and visitors engaged in activities under the Yinson Group.

The Group Chief Executive Officer of Yinson Holdings Berhad is accountable to the Board of Directors for ensuring that this policy is implemented in its entirety.

This Policy will be reviewed every two years or as required.

1 CHAPTER I: OBJECTIVES AND DEFINITION

1.1 Objective & Scope

(a) This Policy shall establish a framework for the responsible management of Personal Data and ensure Yinson Group's compliance with all applicable data privacy laws.

(b) This Policy applies to all Yinson Employees of Yinson Group. All employees (permanent or temporary) must make sure they are familiar with the content of this Policy and comply at all times with the procedures set out in this Policy when handling Personal Data.

(c) Under the terms of their contract with Yinson group of companies ("Yinson Group"), all Yinson Employees who have been authorised access to Personal Data are responsible for handling Personal Data and maintaining confidentiality appropriately at all times.

(d) This Policy may be subject to change and be amended at any time. Any breach of this Policy will be taken very seriously and employees who act outside the requirements or guidance set out in this policy will be asked to explain the reasons for their actions and may face disciplinary action. Wilful and negligent non-adherence to this policy by any employee is a serious disciplinary matter which may result in the employee being be subject to disciplinary action up to and including dismissal.

1.2 Ownership

This Policy and its sub-documents belong to the **Chief Data Privacy Officer** (or his delegate) and shall not be altered without signed Approval.

The procedure is applicable for all Yinson Group's managed documents.

1.3 Abbreviations & Definitions

The Definitions below are the Yinson Group's standard for all managed documents.

YHB	Yinson Holdings Berhad
Data Protection/Privacy	means the sum of all actions taken to protect the personal rights of Data Subjects when handling their Personal Data;
Data Subjects	means all individuals whose personal data are processed within Yinson, including current, future and former employees, customers, suppliers and other contractual partners and interested persons;
Data Protection/ Privacy Authority	means independent public authorities that supervise, through investigative and corrective powers, the application of the relevant data protection/privacy law. They provide expert advice on data protection/privacy issues and handle

	complaints lodged against violations of the data protection/privacy law and the relevant national laws.
DPO	means the Data Protection Officer(s) and/or the person(s) officially named from time to time to monitor internal data protection/privacy issues in Yinson Group;
Individual	means a natural person, whether living or deceased;
Personal Data	means data, in accordance with the provisions under the relevant data privacy legislation. Any processing of Personal Data shall be any operation performed on personal data, such as collecting, creating, recording, structuring, organising, storing, retrieving, accessing, using, seeing, sharing, communicating, disclosing, altering, adapting, updating, combining, erasing, destroying or deleting personal data, or restricting access or changes to personal data or preventing destruction of the data.
Personal Data Protection Assessment	means an assessment of Yinson Employee's knowledge on matters relating to personal data protection;
Yinson Employee	includes permanent worker, temporary worker, trainees of the Yinson Group;

2 CHAPTER II: APPLICATION OF NATIONAL/TRANSNATIONAL LAWS

2.1 Application of National Data Privacy Laws

This Data Privacy Policy does not replace the existing national/transnational laws and instead supplements the various national/transnational data privacy laws. The relevant national/transnational law will take precedence in the event that it conflicts with this Data Privacy, or it has stricter requirements than this Policy. The content of this Data Privacy Policy must also be observed in the absence of corresponding national/transnational legislation. The reporting requirements for data processing under national/transnational laws must be observed.

Each Regional DPO of Yinson Group is responsible for ensuring compliance with this Data Privacy Policy and the respective legal obligations of the national/transnational data privacy laws of Yinson entity the Regional DPO is in charge of. If there is reason to believe that legal obligations under any national/transnational data privacy laws contradict the duties under this Data Privacy Policy, the relevant Regional DPO must inform the Chief DPO. In the event of conflicts between national/transnational legislation and the Data Privacy Policy, the Yinson Data Privacy Team will work together to find a practical solution that meets the purpose of the Data Privacy Policy.

3 CHAPTER III: DATA PRIVACY TEAM STRUCTURE

3.1 Yinson Group Data Privacy Team Structure

The Chief Data Privacy Officer ("Chief DPO") works towards the compliance with national and international data privacy laws for the whole of Yinson Group of Companies. The Chief DPO is responsible for the overseeing of Yinson's implementation of data privacy policies and monitoring worldwide compliance of the relevant data privacy laws. In general, all the various entities of Yinson Group in their respective country/jurisdiction are required to appoint a Regional Data Privacy Officer ("Regional DPO"). These Regional DPOs shall be in charge of managing compliance of their respective jurisdictions' data privacy laws

The Regional DPOs shall promptly inform the Chief DPO of any data protection/privacy risks/breaches and/or any updates to their jurisdictions data privacy laws accordingly.

Any Data Subject may approach the relevant Regional DPOs, at any time to raise concerns, ask questions, request information or make complaints relating to data protection/privacy or data security issues. If requested, concerns and complaints will be handled confidentially.

If the Regional DPO in question cannot resolve a complaint or remedy a breach of the Policy for data protection/privacy, the Chief DPO must be consulted immediately. Decisions made by the Chief DPO to remedy data protection/privacy breaches must be discussed and approved by the senior management of Yinson Group. Inquiries by supervisory authorities must always be reported to the relevant Regional DPO and the Chief DPO.

3.2 Chief Data Privacy Officer

The Chief DPO shall have the following tasks:

a) Responsible for informing and advising the Yinson Group and its employees of their obligations pursuant to this Data Privacy Policy;

b) Monitoring compliance with the Data Privacy Policy and the relevant sub-policies, and all relevant data privacy laws and regulations;

c) Overall responsibility for ensuring awareness-training and training of Yinson Employees;

d) Coordinate and participate in Data Protection Impact Assessments and group risk assessments, provide advice where requested and follow up on actions from assessments;

e) Conduct yearly review and update of the Data Privacy Policy

f) Deal with Regional DPOs and monitor progress of implementation of Data Privacy policies across Yinson Group

g) Reporting to the General Counsel in relation all Data Privacy status issues of Yinson Group.

3.3 Regional Data Privacy Officer

The Regional DPOs shall have the following tasks:

a) Handling local complaints from Data Subjects, access requests and other requests from Data Subjects related to the exercise of their individual rights;

b) General reporting and reporting privacy issues to the Chief Data Privacy Officer;

c) Ensure local communication to Data Subjects and others;

d) Follow-up and monitor changes in local laws and regulations and inform Group Privacy Officer when necessary;

e) Co-operating with and being key contact point for the competent DPA and dealing with DPA investigations;

f) Plan, authorize and arrange necessary training for target groups and Yinson Employees in the DPO's relevant jurisdiction;

g) Prepare annual compliance program for monitoring compliance;

h) Deals with Personal Data Breach in cooperation with the Chief DPO;

i) Ensuring Data Privacy compliance at a DPO's jurisdiction; and

j) Co-operating with local Data Protection/Privacy Authorities ("DPA").

4 CHAPTER IV: DATA PRIVACY PRINCIPLES

The following general principles are primarily based on the data privacy laws of Singapore and Malaysia and further details may be set out in data privacy and information security global procedures applicable to all Yinson entities in the various jurisdictions.

Any inquiries concerning the general principles should be addressed to the relevant Regional DPOs.

NOTE: Consent is not required if it is deemed permissible to obtain/process/disclose such Personal Data under other legal basis pursuant to the relevant national/transnational data privacy legislation.

4.1 Consent

a) Yinson Group shall not collect, use, or disclose any Data Subject's Personal Data without obtaining the Data Subject's consent.

b) Unless permitted elsewhere in this Policy, Yinson Group shall not require a Data Subject to consent to the collection, use, or disclosure of any Personal Data beyond what is reasonably necessary.

c) Yinson Group shall not obtain a Data Subject's consent using false information or misleading practices.

d) Yinson Group may also collect, use, or disclose Personal Data from a Data Subject where permitted, required or authorised under the relevant data privacy law or any other written law. This includes instances where:

   i) The collection, processing, or disclosure of the Personal Data is necessary in the legitimate interest of the Data Subject or the legitimate interests of a third party, unless there is a good reason to protect the Personal Data which overrides those legitimate interests;

   ii) The collection, use, or disclosure of the Personal Data is necessary in the national/public interest, or for any investigations of proceedings;

   iii) The Personal Data is publicly available;

   iv) The Personal Data is necessary for evaluative purposes; and

   v) The Personal Data is collected in the course of employment with Yinson Group and is reasonably necessary for purposes of managing or terminating the Data Subject's employment.

   vi) The collection, processing, or disclosure of the Personal Data is necessary for the performance of contract with the Data Subject, or because the Data Subject has requested take specific steps before entering into a contract.

   vii) The collection, processing, or disclosure of the Personal Data is necessary to protect someone's life.

   viii) The collection, processing, or disclosure of the Personal Data is necessary to comply with the law (not including contractual obligations)

e) For documentation purposes, statements of consent shall generally be obtained either in written or electronic form.

f) In certain situations, consent may be given verbally, in which case the consent shall be properly documented.

i) The statement of consent should indicate that the Data Subject has been notified of the purpose for which the Personal Data will be collected, used, or disclosed.

4.2 Collection of Personal Data

a) Yinson Group shall collect a Data Subject's Personal Data only for purposes which would be considered reasonably appropriate and necessary for the purposes disclosed to the Data Subject, and where the Data Subject has been informed of and has consented to the purpose.

b) Yinson Group may collect Personal Data in the following instances, but not limited to:

i) When a Data Subject performs a transaction with Yinson Group;

ii) When a Data Subject accesses the Yinson Group's website;

iii) When a Data Subject submits a job application to the Yinson Group;

iv) When a Data Subject asks to be included in the Yinson Group's mailing list;

v) When a Data Subject requests that the Yinson Group contact the Data Subject;

vi) When a Data Subject requests for information; and

vii) When a Data Subject submits his Personal Data to the Yinson Group for any other reason.

c) Prior to obtaining consent for the collection of a person's Personal Data, the Yinson Group or its employees shall seek to inform the Data Subject of the following information:

i) The identity of the collector of the Personal Data;

ii) The purpose for which the Personal Data is being collected;

iii) Any other purpose the Personal Data may be used for; and

iv) The third parties or categories of third parties to whom the Personal Data may be transferred.

4.3 Storage and Protection of Personal Data

The following security measures are non-exhaustive and shall be detailed further under the Yinson Information Security Policy.

a) Yinson Group shall record all Personal Data in an accurate and complete manner.

b) Yinson Group shall make reasonable effort to ensure that all Personal Data is correct and up to date, particularly where:

i) The Personal Data is likely to be used by Yinson Group to make a decision that affects the Data Subject concerned; and

ii) The Personal Data is likely to be disclosed by Yinson Group to third parties.

c) All Personal Data collected by Yinson Group shall be stored in a secure and organised manner to prevent unauthorised access, loss, or modification. The following security measures are recommended to be implemented as follows:

i) Personal Data shall be treated and labelled as confidential and shall only be accessible to authorised Yinson Employees who require such data for the fulfillment of their duties, and only to the extent necessary for the scope of the task in question.

ii) Paper files and other physical documents containing Personal Data shall be kept in a secure environment.

iii) Personal Data held on computers and computer systems shall be protected by appropriate software and technology.

iv) Where Personal Data is protected by password, such passwords shall be secure, private, and regularly changed, and shall not be shared or easily compromised. It is recommended to use passwords for access to personal emails and internal systems which must be unique and must not be used on other external systems or services. For example, passwords for personal emails must not be used for personal passwords used to access knowledge base systems of Yinson Group.

d) <u>Offices Entry Control</u>

Yinson Group offices entry control are, but not limited to, the following:

i) If any Yinson Employee identifies an unknown, un-escorted or otherwise unauthorized individual in the office premises, the Yinson Employee shall immediately notify the DPO accordingly.

ii) Visitors to any Yinson Group office must be escorted by an authorized employee at all times. If any Yinson Employee is responsible for escorting visitors, he or she must restrict them to the permitted appropriate areas of the office premise.

iii) Renovation workers and other maintenance workers are required to be monitored at all times.

e) <u>Desks and Workstations</u>

i) Yinson Employees must ensure that documents or devices containing Personal Data, such as company laptops, are not left unduly exposed, for example at a meeting with client in office meeting rooms.

ii) Paper records containing Personal Data must always be stored securely unless in use and should not be left on desks or other areas accessible by third parties.

iii) Electronic records containing Personal Data:

I. must either be encrypted or must be kept on devices which have their hard drives encrypted;

II. must be kept in separate folders to electronic files not containing Personal Data;

III. must only be transferred from desktop computers to portable devices if absolutely necessary. Records may only be put onto portable devices or media such as CDs, USB memory sticks or laptops if the device itself and/or the records are encrypted. Desktop computers and laptops on which electronic records are stored or accessed must be running an up-to-date operating system and up-to-date firewall and anti-virus software.

f) Working outside of Yinson Group office premises

i) Yinson Employees must ensure that documents or devices containing Personal Data, such as company laptops, are not left unduly exposed outside of office premises, for example at a meeting with client.

ii) At all times where reasonably possible, keeping all files and documents containing Personal Data on-site, or where a specific business need requires off-site working, encrypted memory sticks and password protected access should always be used.

iii) Yinson Employees should ensure that their computer monitors do not show any form of Personal Data or confidential information to passers-by and that employees log off from or lock their computers before leaving them unattended.

4.4 Use/Processing of Personal Data

a) Yinson Group shall use/process a Data Subject's Personal Data only for purposes which would be considered reasonably appropriate and necessary for the purposes disclosed to the Data Subject, and where the Data Subject has been informed of and has consented to the purpose.

b) Before accessing and using/processing a Data Subject's Personal Data, Yinson Group shall check the following:

i) Whether the purpose for which the Personal Data is to be used/processed has been consented to by the Data Subject;

ii) Whether the Data Subject's consent has been withdrawn, or is the subject of a withdrawal of consent request; and

iii) The extent to which the use/processing of the Personal Data is necessary for the intended purpose.

c) Where a Data Subject has consented to having his Personal Data used/processed for the purposes as intended and notified expressly to the Data Subject:

i) The Personal Data may be used/processed for the purposes as expressly notified to the Data Subject; and

ii) Yinson Group may contact the Data Subject using his Personal Data for the purpose of communication in relation to the purposes as expressly notified to the Data Subject;

d) Where the use/processing of the Personal Data is otherwise authorised or required under any data privacy law or any other written law:

i) Yinson Group shall first ascertain that the use/processing of the Personal Data is in fact authorised or required, such as in the national interest, in the Data Subject's interest, or in for the purpose of investigations; and

ii) Yinson Group shall only use/process the Personal Data to the extent permitted or required, and in compliance with the relevant statutes or regulations.

e) All use/processing of Personal Data shall be conducted in an organised and secure manner.

f) Personal Data shall only be processed by authorised Yinson Employees who have received adequate training/education in the proper management of Personal Data.

g) Personal Data shall be processed in accordance with formalised procedural guidelines for the management and handling of Personal Data.

h) Personal Data shall be kept private and confidential throughout processing.

4.5 Transmission of Personal Data

a) In the course of business, it may be necessary for Yinson Group to disclose or transmit Personal Data, both within the organisation and to external third parties.

b) Yinson Group shall disclose a Data Subject's Personal Data only for purposes which would consider reasonably appropriate and necessary for the purposes disclosed to the Data Subject, and where the Data Subject has been informed of and has consented to the purpose.

c) Before transmitting a Data Subject's Personal Data, Yinson Group shall check the following:

i) Whether the purpose for which the Personal Data is to be transmitted has been consented to by the Data Subject;

ii) The extent to which the processing of the Personal Data is necessary for the intended purpose; and

iii) Whether the transmission is in conflict with any interest of the Data Subject that merits protection.

d) If the Personal Data is to be transmitted to a third party outside of the relevant jurisdiction/country under which the data was received form the Data Subject ("Host Country"), Yinson Group shall:

i) Obtain sufficient contractual undertaking from that the said third party that the Personal Data shall be subject to a level of Data Protection in line with this Policy; or

ii) Otherwise ensure that the Personal Data shall be managed in accordance with the requirements of the privacy laws of the Host Country.

e) All Personal Data disclosed/transmitted to a third party shall be pursuant to the relevant Data Protection clauses and/or agreements that the Yinson Data Privacy Team/Legal Team have put in place.

f) It must be remembered that if the Personal Data is transmitted to a third-party service provider for use/processing, the security of the Personal Data remains the responsibility of Yinson Group. When selecting a third-party service provider, Yinson Group shall thus ensure that:

i) The service provider is capable of ensuring the necessary technical and organisational requirements to adequately protect the Personal Data;

ii) The service provider shall only process the Personal Data in accordance with Yinson Group's instructions;

iii) The service provider's compliance undertaking with the relevant Personal Data security and other requirements shall be included in its contract with Yinson Group.

iv) Yinson Group retains full responsibility for correct performance of the Personal Data processing.

v) Before issuing the order, the following requirements must be complied with;

I. The third-party service provider must be chosen based on its ability to cover the required technical and organizational protective measures.

II. The order must be placed in writing. The instructions on data processing and the responsibilities of the client and provider must be documented.

III. Before data processing begins, the Yinson Group must be confident that the provider will comply with the duties imposed. For example, the third-party service provider may document its compliance with data security requirements in particular by presenting suitable certification. Depending on the risk of data processing, the reviews must be repeated on a regular basis during the term of the contract with the third-party service provider.

g) In the case that Personal Data is transmitted to Yinson Group by a third party, Yinson Group shall ensure that:

i) The Personal Data has been collected by the third party in accordance with the relevant legal provisions; and

ii) The Data Subject has consented to the transmission and use of his Personal Data for the intended purpose.

h) All transmission of Personal Data shall be conducted in an organised and secure manner.

i) Personal Data shall only be transmitted by authorised Yinson Employees who have received adequate training in the proper transmission of Personal Data.

j) Personal Data shall be transmitted in accordance with formalised procedural guidelines for the transmission and disclosure of Personal Data.

k) Personal Data shall be kept private and confidential throughout transmission.

l) Personal Data that must be transferred within Yinson Group is to be transferred only via business provided secure transfer mechanisms, such as encrypted USB keys, file shares, email. Yinson Group will provide Yinson Employees with systems or devices that fit this purpose. Authorized Yinson Employees must not use other mechanisms, such as personal email account, to handle in such data. If Yinson Employees have a query regarding use of a transfer mechanism, they are to contact the relevant Regional DPO for clarification.

m) Any information being transferred on a portable device, such as an USB stick or laptop, must be encrypted in line with industry best practices and applicable law and regulations. If Yinson Employees have any doubts regarding the requirements, they are to seek guidance from the relevant Regional DPO.

n) Yinson Employees are required not to reference the subject or content of sensitive or confidential data publicly, or via systems or communication channels not controlled by Yinson Group. For example, the use of external e-mail systems not hosted by Yinson Group to distribute data is not allowed.

4.6 Retention of Personal Data

a) Yinson Group shall not keep Personal Data indefinitely. Yinson Group shall cease to retain Personal Data when:

   i) The purpose for which the Personal Data was collected is no longer being served; or

   ii) Retention is no longer necessary for relevant business or legal purposes.

b) Personal Data shall be retained for periods including the following:

   i) Personal Data of third parties: (After the purpose/contract has expired) Proposed time frame can range from 6 months to 5 years (the relevant Department should determine the reasonable appropriate retention period).

   ii) Personal Data of Yinson Employees (after they have left the Yinson Group): 7 years (the relevant HR Department should determine the reasonable appropriate retention period). After the Yinson Employee have left employment, all portions of Personal Data that Yinson has no purpose or reason to use/store/disclose, have to be deleted/not retained. Only the portions of Personal Data that Yinson can establish a valid purpose/reason to use/store/disclosed shall be retained.

      I. Examples of Personal Data that can be retained after Yinson Employees have left: Employee travel details/Salary payment details for Finance audit purposes)

      II. Examples of Personal Data that cannot be retained after Yinson Employees have left: Employee Photographs, Marriage Details, Educational and Professional Certificate copies)

iii) All Personal Data retained is only for purposes as notified to the relevant Data Subjects. Any Personal Data that are not required for these purposes should not be retained unless where reasonable under the relevant national/transnational privacy laws, or where required under any other written law.

c) When Yinson Group ceases to retain any Personal Data, such Personal Data shall be removed or deleted in a secure and permanent manner, or else properly anonymised to prevent further use.

d) Deletion or anonymisation of Personal Data shall be conducted in an organised and secure manner.

e) Personal Data shall only be deleted or anonymised by authorised Yinson Employees who have received adequate training in the proper deletion or anonymisation of Personal Data.

f) Personal Data shall be deleted or anonymised in accordance with formalised procedural guidelines for the transmission and disclosure of Personal Data.

g) Personal Data shall be kept private and confidential throughout deletion or anonymisation.

h) No paper document containing Personal Data should be used as wastepaper or left in bins or be brought outside of office premises. These paper documents containing Personal Data are to be shredded manually and disposed properly.

i) Non-rewritable media, such as non-rewritable CDs, containing electronic documents should be physically destroyed when they are no longer required or if such media is damaged and/or will not be used again.

j) Terminated and resigned Yinson Employees will be required to return all records, in any format, containing personal information. This requirement should be part of the Yinson Employee onboarding process with Yinson Employees signing the letter of appointment to confirm they will do this.

k) Yinson Employees with re-designated positions may be required to hand over all records containing Personal Data if such possession of the relevant Personal Data is no longer required in the re-designated role.

4.7 Personal Data Requests

The rights of Data Subjects listed below. These are the minimum rights made available to Data Subjects but are non-exhaustive list and supplements additional rights available to Data Subjects under the various national/transnational Data Privacy legislation.

<u>Access Request</u>

a) A Data Subject may request to be provided with all Personal Data about that Data Subject that is within Yinson Group's possession, as well as information about how that data has been used or disclosed within a year before the request.

b) Data Subjects may submit an access request in relation to their Personal Data to the relevant DPO.

c) Yinson Group shall endeavour to attend to all Personal Data access requests within 30 days, or within a period which is reasonable under the circumstances or as specified by the relevant national/transnational data privacy laws.

d) Yinson Group shall not accede to a request where the provision of such data or information is not authorised or required under the PDPA or any other written law, or where the request is frivolous, vexatious, or may cause unreasonable interference with Yinson Group's operations.

e) Yinson Group may charge a certain agreed fixed fee (as reasonably permitted) for the cost and time of attending to the access request provided that such a charge has been clearly notified to the Data Subject making the request.

Amendment Request

f) A Data Subject may request Yinson Group to amend and/or correct an error or omission in his Personal Data that is within Yinson Group's possession.

g) Data Subjects may submit a Personal Data amendment/correction request Form to the relevant DPO.

h) Yinson shall conduct measures to verify the details of amendments/correction before proceeding accordingly.

i) Yinson Group shall endeavour to attend to all requests within 30 days, or within a period which is reasonable under the circumstances or as specified by the relevant national/transnational data privacy laws.

j) Yinson Group shall correct the Personal Data as soon as practicable, and shall, where necessary, send the amended/corrected Personal Data to any organisation the data was disclosed to within a year before the request.

k) Yinson Group shall not accede to a request where the correction is not authorised or required under the relevant data privacy law or any other written law, or where there are reasonable grounds why the amendment/correction should not be made.

Withdrawal Request

l) A Data Subject may withdraw consent to the collection, use, or disclosure of his Personal Data upon the provision of reasonable notice to Yinson Group.

m) Data Subjects may submit a withdrawal of consent notification to the relevant DPO.

n) Yinson Group shall endeavour to attend to all requests within 30 days, or within a period which is reasonable under the circumstances or as specified by the relevant national/transnational data privacy laws.

o) Yinson Group shall notify the Data Subject of the consequences of withdrawal of consent, and shall cease to collect, use, or disclose the Data Subject's personal information upon processing of the notice of withdrawal within 30 days or as specified by the relevant national/transnational data privacy laws.

p) Yinson Group shall notify the Data Subject of the consequences of withdrawal of consent, and shall cease to collect, use, or disclose the Data Subject's personal information upon processing of the notice of withdrawal within 30 days or as specified by the relevant national/transnational data privacy laws.

4.8 Rights of the Data Subject

Every Data Subject has the following rights. Their assertion is to be handled immediately by the responsible Yinson unit and cannot pose any disadvantage to the Data Subject. The rights of Data Subjects are listed below. These are the minimum rights made available to Data Subjects but are non-exhaustive list and supplements additional rights available to Data Subjects under the various national/transnational Data Privacy legislation.

a) The Data Subject may request information on which Personal Data relating to him/her has been stored, how the data was collected, and for what purpose. If there are further rights to view the employer's documents (e.g. personnel file) for the employment relationship under the relevant employment laws, these will remain unaffected.

b) If Personal Data is transmitted to third parties, information must be given about the identity of the recipient or the categories of recipients.

c) If Personal Data is incorrect or incomplete, the Data Subject can demand that it be corrected or supplemented.

d) The Data Subject can object to the processing of his or her data for purposes of advertising or market/opinion research. The data must be blocked from these types of use.

e) The Data Subject may request his/her data to be deleted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed.

f) The Data Subject generally has a right to object to his/her data being processed, and this must be taken into account if the protection of his/her interests takes precedence over the interest of the data controller owing to a particular personal situation. This does not apply if a legal provision requires the data to be processed.

5 CHAPTER V: AWARENESS AND EDUCATION

5.1 Awareness and Education

a) All Yinson Employees are to be familiar with Personal Data security and compliance awareness and pass the Personal Data Protection Assessment e-learning course or other Data Privacy Assessments as designated by the respective regional DPOs. The aim of appropriate training is to make the Data Privacy Policy known, understood and effectively applied throughout the Yinson Group.

b) A special training program is available/shall be made available for all Yinson Employees. The special training program involves basic courses based on online electronic learning explaining the principles set out in the Data Privacy Policy and involving guidelines for processing of Personal Data. The relevant Regional DPO shall organize and schedule the relevant training program for the Yinson Employees in their respective jurisdictions.

c) Further, all Yinson Employees have at all times the relevant information available online via the Yinson Group intranet and combined with information presented via relevant communication channels to create awareness among all Yinson Employees of individual rights and duties considering processing of Personal Data.

6 CHAPTER VI: DATA BREACH AND RESPONSE

6.1 Types of Personal Data Breach

a) A Personal Data breach is a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed".

b) A breach is therefore a type of security incident and there are three different types of breach that may occur:

i) Confidentiality breach – an accidental or unauthorised disclosure of, or access to, Personal Data.

ii) Availability breach – an accidental or unauthorised loss of access to, or destruction of, Personal Data.

iii) Integrity breach – an accidental or unauthorised alteration of Personal Data.

A breach can concern confidentiality, availability and integrity of Personal Data at the same time, as well as any combination of these.

6.2 Causes of Data Breach

a) Data breaches may be caused by Yinson Employees, parties external to the organization, or computer system errors. The following are not an exhaustive list.

<u>Human Error</u>

b) Human Error causes include:

i) Loss of computing devices (portable or otherwise), data storage devices, or paper records containing Personal Data

ii) Disclosing data to a wrong recipient

iii) Handling data in an unauthorized way (e.g.: downloading a local copy of Personal Data)

iv) Unauthorized access or disclosure of Personal Data by employees (e.g.: sharing a login)

v) Improper disposal of Personal Data (e.g.: hard disk, storage media, or paper documents containing Personal Data sold or discarded before data is properly deleted)

<u>Malicious Activities</u>

c) Malicious causes include:

i) Hacking incidents / Illegal access to databases containing Personal Data

ii) Theft of computing devices (portable or otherwise), data storage devices, or paper records containing Personal Data

iii) Actions that cause/influence any Yinson Employee into releasing Personal Data of Data Subjects

d) Computer System Error

Computer System Error causes include:

i) Data breaches may be caused by employees, parties external to the organization, or computer system errors.

ii) Errors or computer virus/bugs in any software used by Yinson Group.

iii) Failure of cloud services, cloud computing or cloud storage security / authentication / authorization systems.

iv) In the event that any Yinson Employee finds a system, process, or colleague, which or who is suspected to be not compliant with this Data Privacy Policy, the said employee has a duty to inform the DPO so that appropriate action can be taken.

6.3 Data Breach Reporting Procedure

a) All Yinson Employees have an obligation to report actual or potential Data Protection/Privacy compliance failures. This allows Yinson Group to:

i) Investigate the failure and take remedial steps if necessary;

ii) Maintain a register of compliance failures;

iii) Notify the relevant DPA of any compliance failures that are material either in their own right or as part of a pattern of failures.

iv) Evaluate the remedial action taken.

b) If any Yinson Employee knows or suspects that a Personal Data breach has occurred, the Yinson Employee must immediately both advise their department head and contact the relevant DPO. The said Yinson Employee must ensure to retain any evidence in relation to the breach and must provide a written statement setting out any relevant information relating to the actual or suspected Personal Data breach, including:

i) name, department and contact details;

ii) the date of the actual or suspected breach;

iii) the date of discovery of the actual or suspected breach;

iv) the date of statement report;

v) a summary of the facts relating to the actual or suspected breach, including the types and amount of Personal Data involved;

vi) what is believed to be the cause of the actual or suspected breach;

vii) whether the actual or suspected breach is ongoing;

viii) who is believed to be affected by the actual or suspected breach.

Yinson Employees must then follow the further advice of the relevant DPO. Yinson Employees must never attempt to investigate the actual or suspected breach by themselves and must not attempt to notify affected Data Subjects. The relevant DPO, with other nominated Yinson Employees, will investigate and assess the actual or suspected Personal Data breach in accordance with the response plan set out below and will determine who should be notified and how. A template can be found at Annexure A (Incident Response Form) of the Information Security Policy to assist in documenting the required information.

Response plan

a) The Chief DPO and/or the relevant Regional DPO will assemble a team to investigate, manage and respond to the Personal Data breach. They will lead this team and the other members will consist of nominated senior members of the management team. The data breach team will then:

   i) Make an urgent preliminary assessment of what data has been lost, why and how.

   ii) Take immediate steps to contain the breach and recover any lost data.

   iii) Undertake a full and detailed assessment of the breach.

   iv) Record the breach in the Yinson Groups' data breach register.

   v) Notify the relevant DPA where the breach is likely to result in a risk to the rights and freedoms of Data Subjects.

   vi) Notify affected Data Subjects where the breach is likely to result in a high risk, (as deemed by the relevant DPO), to their rights and freedoms.

   vii) Respond to the breach by putting in place any further measures to address it and mitigate its possible adverse effects, and to prevent future breaches.

Notification to the respective DPAs

b) Not all Personal Data breaches have to be notified to the DPA. The breach will only need to be notified if it is likely to result in a risk to the rights and freedoms of data subjects, and this needs to be assessed by the relevant DPO on a case-by-case basis.

c) Where a breach is reportable, the relevant DPO must notify the DPA without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. If our report is submitted late, it must also set out the reasons for our delay. The notification must at least include:

   i) a description of the nature of the breach including, where possible, the categories and approximate number of affected data subjects and the categories and approximate number of affected records;

   ii) the name and contact details of the relevant DPO;

   iii) a description of the likely consequences of the breach;

   iv) a description of the measures taken, or to be taken, by Yinson Group to address the breach and mitigate its possible adverse effects.

The above information can be provided in phases, without undue further delay, if it cannot all be provided at the same time. A template can be found at Annexure B (Data Breach Response Form) of the Information Security Policy.

d) Awareness of the breach occurs when we have a reasonable degree of certainty that a breach has occurred. In some cases, it will be relatively clear from the outset that there has been a breach. However, where it is unclear whether or not a breach has occurred, Yinson Group will have a short period of time to carry out an initial investigation after first being informed about a potential breach in order to establish with a reasonable degree of certainty whether or not a breach has in fact occurred. If, after this short initial investigation, it can be established that there is a reasonable degree of likelihood that a breach has occurred, the 72 hours starts to run from the moment of that discovery.

Communication to affected Data Subjects

e) Where the Personal Data breach is likely to result in a high risk (as deemed by the relevant DPO) to the rights and freedoms of Data Subjects, Yinson Group also needs to communicate the breach to the affected Data Subjects without undue delay, i.e. as soon as possible and in clear and plain language provide them with:

i) a description of the nature of the breach;

ii) the name and contact details of the relevant DPO;

iii) a description of the likely consequences of the breach;

iv) a description of the measures taken, or to be taken, by Yinson Company to address the breach and mitigate its possible adverse effects.

f) However, Yinson Group does not need to report the breach to Data Subjects if:

i) there has been implementation of appropriate technical and organisational protection measures, and those measures have been applied to the Personal Data affected by the breach, in particular those that render the Personal Data unintelligible to any person who is not authorised to access them, such as state-of-the-art encryption, or

ii) subsequent measures have been taken to ensure that the high risk to the rights and freedoms of Data Subjects is no longer likely to materialise.

Data breach register

g) Yinson Group will maintain a register of all Personal Data breaches, regardless of whether or not they are notifiable to the relevant DPA. The register will include a record of:

i) the facts relating to the breach, including the cause of the breach, what happened and what Personal Data were affected;

ii) the effects of the breach;