



HEXTAR HEALTHCARE BERHAD
(formerly known as Rubberex Corporation (M) Berhad)
199601000297 (372642-U)

PERSONAL DATA PROTECTION POLICY

Personal Data Protection Notice

The personal data that we process and/or will process may include your name, contact details, email address, home address and mailing address and any other personal data derived from any documentation.

Subject to the relevant laws in Malaysia i.e., the Personal Data Protection Act 2010 (“the Act”), we may use your personal data for the following purposes:

- a. to enable us to discharge our contractual obligations;
- b. for data processing or reporting purposes;
- c. to comply with any legal and/or regulatory requirements;
- d. for billing and financial purposes, accounting and tax;
- e. to respond to your enquiries or complaint;
- f. to provide marketing materials about events, services and products;
- g. for contact purposes; and
- h. for any other purpose that is permitted by law and regulations.

Your personal data is collected from various sources, including information you may have provided us, information from third parties and information in the public domain. We may transfer your personal data to our related entities or external service providers outside Malaysia for the above purposes.

Subject to the requirement under the Act, if you would like to make any enquiries or complaints or request access or correction of your personal data, please contact us in writing using any of the following modes:

Mailing Address: Lot 138201 Off ¼ Mile Jalan Bercham, Kawasan Perindustrian Bercham,
31400 Ipoh, Perak, Malaysia

Email Address: info_hexcare@hextar.com

We may disclose your personal data to the following parties for the purposes stated above:

- a. our subsidiaries, related and associated companies;
- b. the supervisory, governmental or relevant authority;
- c. auditors, solicitors, professional advisors, insurer and financial institutions; and
- d. any person which we may engage for the purpose of performing or in connection with the performance of services or operational functions which have been out-sourced.

You hereby consent to the processing of your personal data in accordance with all of the foregoing. We will seek your consent before using your personal data for purposes other than those stated above.

Data Retention

General Rule: Personal data processed for any purpose(s) will not be kept longer than is necessary for the fulfilment of that purpose.

- 1 It is the Company's duty to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed.
- 2 We will review the personal data which we hold on a regular basis and delete any data which are no longer required in connection with the purpose for which they were originally obtained. When carrying out this exercise we will consider any legal or other requirements to retain data.
- 3 We will also consider the type of relationship which the Company has with the data subject and whether there is an expectation that we will retain data for any given period of time (e.g. employees' data will have to be retained for a period of at least seven(7) years after they had left the employment of the Company and accounting records and business transactions should be retained for at least seven(7) years).
- 4 Personal data used for marketing purposes may be retained for as long as required if the data protection notice has obtained the necessary consent to process the personal data for marketing purposes indefinitely. However, the Company will promptly remove permanently or restrict the manner of processing the data for marketing purposes if there are complaints and requests for restriction of the manner the Company processes the personal data.
- 5 Based on the above, it is the Company's general policy to retain personal data for at least seven(7) years after the purpose for which the personal data were originally obtained have been carried out or for such further period as is necessary for the purposes of compliance with relevant laws.

Data Security

- 1 The Company must when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.
- 2 The Security Principle requires the Company to develop and implement technical and organizational measures to protect personal data which we process:-
 - (a) technical measures may include software controls to restrict user access; up-to-date protection against malicious software and viruses; backing up of data; network access control; audit trail software; disaster recovery; secure destruction or deletion of data and secure disposal of computer equipment and removable media; user authentication; guidance on teleworking and mobile computing; encryption and all of which we have in place and manage through our information systems.
 - (b) organisational measures may include restricting access to buildings and computer rooms; ensuring secure disposal of information; and training staff on the care and handling of personal data and all of which we are responsible for complying with and applying to our daily routine.
- 3 This principle imposes upon the Company additional obligations if we use third parties to process personal data on our behalf. Examples of these third parties may include vendors and disaster recovery services. Some of these third parties may have access to or need to process personal data on our behalf. If so, they will be acting as our data processors and the Act requires us to:-
 - (a) ensure that the data processor provides sufficient guarantees in respect of the technical and organizational security measures governing the processing to be carried out; and
 - (b) take reasonable steps to ensure compliance with those measures.

For this purpose, we are required to:-

 - (i) put in place a contract in writing with each of our data processors under which they agree to act only on instructions from us;
 - (ii) include the right to audit our data processors to ascertain compliance with the data protection requirements of the processing contract; and/or
 - (iii) ensure that the data processor agrees to comply with obligations equivalent to those imposed on us by the Security Principle by way of an executed Letter of Undertaking by the data processor.
- 4 If you are responsible for the selection, appointment or use of data processors, you must ensure that you only select those processors that are able to provide us with sufficient guarantees in respect of the technical and organisational measures that will apply to the processing of our personal data. Furthermore, if you are responsible for

the drafting or negotiation of contracts with data processors, you must ensure those contracts contain all applicable data protection provisions. Please seek further advice from the personnel responsible for data protection matters before signing the contract.

- 5 You must ensure that we have the right to check the data processor's compliance with the terms of any processing contract. This may involve auditing the data processor from time to time to make sure that it is processing in accordance with our instructions and the security measures we have specified, as well as any other data protection related requirement of the Act.
- 6 If the data processor will be holding personal data on our behalf and we do not also hold a copy of those data, we must make sure the processing contract includes a provision that requires the processor to assist us promptly with any *subject access request we might receive in relation to any of the personal data held by the data processor.

*A 'subject access request' is a request received from a data subject asking for access to personal data which we process about him or her

- 7 You must ensure that upon termination of the processing contract, the processor promptly returns or destroys the personal data as directed by us.
- 8 If the data processor will be collecting personal data on our behalf, the processing contract must include an obligation upon the processor to give our standard data protection notice (which the processor is not allowed to modify) to all individuals about whom the processor collects personal data.
- 9 It is important to remember that just because we delegate some our processing activities to a data processor does not mean that we can delegate our legal responsibility to comply with the Act. As a data controller, we remain legally liable for the processing of personal data that are under our control, even if the processing activity itself was carried out by a data processor.
- 10 Hard copies of any data collection form and document which contains records of personal data should be secured and locked in a designated area of the Company's premises where a limited number of staffs may have regulated access. These authorised staffs may be required to record their time of arrival and departure as well as the items collected at the designated area.

Data Access / Correction Request

Akses Data / Permintaan Pembedulan

Data access/correction request form for a request made by a data subject

Borang permintaan akses/pembedulan data untuk permintaan yang dibuat oleh subjek data

- 1 Your name (in full)
Nama penuh anda
- 2 Your mobile contact number
Nombor telefon bimbit anda
- 3 Your email address
Alamat e-mel anda
- 4 Your postal address
Alamat sura menyurat anda
- 5 Your [customer number/employee number/identification number]
Nombor pelanggan/nombor pekerja/nombor identifikasi anda
- 6 Please provide a copy of your driving licence, passport or identity card
Sila berikan salinan lesen memandu, pasport atau kad pengenalan anda
- 7 Description of personal data you are requesting and any information you have as to the location of the data (e.g., describe any departments or parts of the organisation where you have worked, or with whom you communicate or have dealings, as appropriate) [as well as the correction sought after]
Perihal data peribadi yang anda minta dan sebarang maklumat yang anda ada tentang lokasi data (cth., terangkan mana-mana jabatan atau bahagian organisasi tempat anda bekerja, atau dengan yang anda berkomunikasi atau berurusan, mengikut kesesuaian) [serta pembedulan yang dicari]
- 8 Please check the information you have provided and sign the form. Kindly send the form to us by any of the following modes:
Sila semak maklumat yang anda berikan dan tandatangani borang tersebut. Sila hantar borang kepada kami melalui mana-mana daripada mod berikut:

Mailing Address: Lot 138201 Off ¾ Mile Jalan Bercham, Kawasan Perindustrian Bercham,
31400 Ipoh, Perak, Malaysia
Alamat Surat Menyurat: Lot 138201 Off ¾ Mile Jalan Bercham, Kawasan Perindustrian Bercham, 31400 Ipoh, Perak,
Malaysia
Email Address: info_hexcare@hextar.com
Alamat E-mel: info_hexcare@hextar.com
- 9 By providing my personal data, I confirm that I have read and understood the Company's privacy notice available on the Company's website at www.hextarhealthcare.com and consent to processing of my personal data for the purposes stated in the privacy notice.
Dengan memberikan data peribadi saya, saya mengesahkan bahawa saya telah membaca dan memahami notis privasi Syarikat yang boleh didapati di laman web Syarikat di www.hextarhealthcare.com dan bersetuju untuk memproses saya data peribadi untuk tujuan yang dinyatakan dalam notis privasi.