FAQ to European Union (EU) General Data Protection Regulation (GDPR)

1. Introduction

Hong Kong Cyberport Management Company Limited 香港數碼港管理有限公司 (or "HKCMCL") is committed to respecting and protecting the privacy of our customers, visitors and website users ("Users" or "you") by observing and ensuring full compliance with the requirements stipulated under the Hong Kong Personal Data (Privacy) Ordinance (or "PD(P)O") as well as the General Data Protection Regulation (GDPR) where applicable.

2. What is GDPR and its Applicability in Cyberport?

General Data Protection Regulation, or the GDPR, has gone into effect on May 25, 2018, and it will have a significant impact on companies that collect and process personal data belonging to data subjects located within the EU member states.

As a result, if you are based in a Member State of European Union during your interactions with HKCMCL, your right would be protected in accordance with the GDPR. However, in case you are in Hong Kong during your interactions with HKCMCL, the Hong Kong PD(P)O will prevail.

3. Data Collection and Use

HKCMCL might collect personal information you provide directly to us or that we may obtain in connection with our offerings, such as tenant applications. The types of personal information we may collect include your name, email address, account username, password and/or responses to security questions, address, phone number, company name and your company related contact details, details regarding your job function, job title, industry sector, payment information, photographs, videos, diagrams, notes, and any other personal information you choose to provide.

When you access or use our Services, we may automatically collect certain information, which could include personal information, such as:

- Log Information, including your Internet Protocol ("IP") address, device

information such as operating system, browser type, access times, pages viewed, etc when navigating to our Services;

- Usage Information: We may collect information about your use of our Services, such as how often the Services are used, the duration, etc;
- Information Collected by Cookies and Other Tracking Technologies; and
- Location Information: We may collect information about the location of your mobile device, when accessing or using one of our mobile applications, upon your consent.

4. Lawful Bases for Processing

The lawful bases for processing are set out in Article 6 of the GDPR. These include[1]:

a) Consent: you have given clear consent for HKCMCL to process your personal data for a specific purpose.
b) Contract: the processing is necessary for a contract HKCMCL has with any individual, or because these individuals have asked HKCMCL to take specific steps before entering into a contract.
c) Legal obligation: the processing is necessary for HKCMCL to comply with the law (not including contractual obligations).
d) Vital interests: the processing is necessary to protect someone's life.
e) Public task: the processing is necessary for HKCMCL to perform a task in the public interest or for HKCMCL official functions, and the task or function has a clear basis in law.
f) Legitimate interests: the processing is necessary for HKCMCL legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect an individual's personal data which overrides those legitimate interests.

5. Protection of Personal Data

HKCMCL ensures the confidentiality, integrity and availability of the personal data that we collected and process, with the following security measures in place:

a) Physical security: access to our data centre, offices and facilities are under strict control and protected with CCTV.
b) Data security: All media containing personal information would be

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protectionregulation-gdpr/lawful-basis-for-processing/

encrypted and will be destroyed under international standard when it is no longer in use.

c) Technology security: Our network follows the industry best practice for secure network infrastructure, and our systems follow strict access policy and installed with technologies including firewall, intrusion detection systems, anti-virus, encryption as well as real time network and system monitoring. Vulnerability scanning as well as ISO27001 compliance certification would also be regularly conducted.

d) Organizational and personnel security would be enforced through regular training and awareness programme on HKCMCL security and privacy policies and standards, to ensure that all employees understand the importance as well as their responsibilities to protect all collected personal data.

6. Access of Personal Data by External Parties

In general, HKCMCL would never share the collected personal data with external parties, unless with legitimate justifications (e.g. with your consent) or HKCMCL is required to make disclosure under any law applicable in or outside Hong Kong.

HKCMCL will not sell, rent or otherwise provide our collected personal information to any third parties for marketing purposes.

However, due to operational needs, vendors supporting HKCMCL operations might have access to the systems storing the collected personal data. If there is operation need for external personnel to have access to system holding the collected personal data, the following safeguards would be in place:

a) The external support personnel could never copy any personal data away from HKCMCL;
b) All external support personnel must sign a Non-Disclosure Agreement before support task can be performed;
c) Operations of external support personal would be under CCTV surveillance.

7. What are Your Data Protection Rights?

HKCMCL would like to make sure you are fully aware of all of your data protection rights under GDPR. Every user is entitled to the following:

- The right to access – You have the right to request HKCMCL for copies of

your personal data. We may charge you a small fee for this service.

- The right to rectification – You have the right to request HKCMCL to correct any information you believe is inaccurate. You also have the right to request HKCMCL to complete the information you believe is incomplete.
- The right to erasure (or "the right to be forgotten") – You have the right to request HKCMCL to erase your personal data, under legitimate circumstances.
- The right to restrict processing – You have the right to request HKCMCL to restrict the processing of your personal data, under legitimate circumstances.
- The right to object to processing – You have the right to object to HKCMCL's processing of your personal data, under legitimate circumstances.
- The right to data portability – You have the right to request HKCMCL to transfer the data that we have collected to another organization, or directly to you, under legitimate circumstances.

Upon receiving your request, HKCMCL commits to respond to you within one calendar month. If you would like to exercise any of these rights, please contact us at noc@cyberport.com.hk.