Question #1 *Topic 1*

In the Asia-Pacific Economic Cooperation (APEC) Privacy Framework, what exception is allowed to the Access and Correction principle?

A. Paper-based records.

B. Publicly-available information.

C. Foreign intelligence.

D. Unreasonable expense.

Suggested Answer: *B*

Community vote distribution

D (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: D

D. Unreasonable expense.

upvoted 1 times

Bhimesh 5 months, 4 weeks ago

24. Such access and opportunity for correction should be provided except
where:
(i) the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question;
Commentary -
in some situations, it may be necessary for organizations to deny claims for access and correction, and this Principle sets out the conditions that must be met in order for such
denials to be considered acceptable, which include: situations where claims would constitute an unreasonable expense or burden on the personal information controller, SUCH AS WHEN claims for access are repetitious or vexatious by nature; cases where providing the information would constitute a violation of laws or would compromise security...

upvoted 1 times

Achatterjee 1 year ago

Agree with D. Section 24 of APEC Framework

upvoted 1 times

Alizade 1 year, 6 months ago

Selected Answer: D

D. Unreasonable expense. The APEC Privacy Framework's Access and Correction principle allows for exceptions when providing access to personal information or making corrections would impose an unreasonable burden or expense on the organization. In such cases, organizations may deny or limit access or correction, provided they can justify the decision as necessary and reasonable.

upvoted 3 times

Question #2 *Topic 1*

How can the privacy principles issued in 1980 by the Organisation for Economic Cooperation and Development (OECD) be defined?

A. Guidelines governing the protection of privacy and trans-border data flows issued in collaboration with the Federal Trade Commission.

B. Guidelines governing the protection of privacy and trans-border data flows of personal data in states that are members.

C. Mandatory rules governing the protection of privacy and trans-border data flows within the European Union.

D. Mandatory rules governing the protection of privacy and trans-border data flows among binding member states.

Suggested Answer: *B*

Community vote distribution

B (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: B

B. Guidelines governing the protection of privacy and trans-border data flows of personal data in states that are members.

upvoted 1 times

Question #3 *Topic 1*

Which concept is NOT an element of Cross Border Privacy Rules (CBPR)?

A. Enforcement by Accountability Agents.

B. Self-assessment against CBPR questionnaire.

C. Consultation with Privacy Enforcement (PE) Authority.

D. Dispute resolution via the Accountability Agent's compliance program.

Suggested Answer: *B*

Community vote distribution

C (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: C

C. Consultation with Privacy Enforcement (PE) Authority.

upvoted 1 times

Bhimesh 5 months, 2 weeks ago

Selected Answer: C

C. Consultation with Privacy Enforcement (PE) Authority.

upvoted 1 times

Bhimesh 5 months, 4 weeks ago

Answer - C

Elements of the CBPR System

The CBPR System consists of four elements: (1) self-assessment; (2) compliance review; (3) recognition/acceptance; and (4) dispute resolution and enforcement.

Self-Assessment Questionnaire for Organizations

The CBPR System relies on an organization's self-assessment of their data privacy policies and practices against the requirements of 2015 APEC Privacy Framework using an APEC- recognized CBPR questionnaire (see para 21). This questionnaire will be provided by the appropriate APEC-recognized Accountability Agent, in accordance with established selection requirements

upvoted 1 times

MMMeo 1 year, 1 month ago

Should be C

upvoted 1 times

Question #4 *Topic 1*

What term is defined by the European Commission to mean any data that relates to an identified or identifiable individual?

A. Personally identifiable information.

B. Sensitive information.

C. Personal data.

D. Identified data.

Suggested Answer: *C*

Community vote distribution

C (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: C

C. Personal data.

upvoted 1 times

Bhimesh 5 months, 4 weeks ago

• Personal Data (EU)

• EU – Any information that could be used on its own or in conjunction with other data to ID an individual.

• GDPR: Personal Data

• "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

upvoted 1 times

Question #5 *Topic 1*

What personal information is considered sensitive in almost all countries with privacy laws?

A. Marital status.

B. Health information.

C. Employment history.

D. Criminal convictions.

Suggested Answer: *B*

Community vote distribution

B (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: B

B. Health information.

upvoted 1 times

Question #6 *Topic 1*

Which jurisdiction was the first to consider IP addresses to be personal information?

A. India.

B. Hong Kong.

C. The United States.

D. The European Union.

Suggested Answer: *D*

Community vote distribution

D (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: D

D. The European Union

upvoted 1 times

Alizade 1 year, 6 months ago

Selected Answer: D

The European Union (EU) was one of the first jurisdictions to consider IP addresses as personal information. The EU's data protection framework, the General Data Protection Regulation (GDPR), which came into effect on May 25, 2018, treats IP addresses as personal data in certain circumstances.

upvoted 1 times

Question #7 *Topic 1*

In the area of human rights, what separates Singapore from many other Asian countries?

A. It is not a member of the Association of Southeast Asian Nations (ASEAN).

B. It has not signed the International Covenant on Civil and Political Rights.

C. It has not adopted the ASEAN Human Rights Declaration.

D. It is not a member of the United Nations.

Suggested Answer: *B*

Community vote distribution

B (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: B

B - International Covenant on Civil and Political Rights (ICCPR).

upvoted 1 times

Bhimesh 5 months, 4 weeks ago

B - International Covenant on Civil and Political Rights (ICCPR).

"The Singaporean government missed yet another opportunity to address many human rights concerns raised by the international community. Singapore can no longer ignore the important civil and political rights that its citizens should enjoy."

Karim Lahidji, FIDH President

The government did not accept any of the 24 recommendations on the abolition of the death penalty, including seven that called for the ratification of the Second Optional Protocol to the International Covenant on Civil and Political Rights (ICCPR).

upvoted 1 times

Question #8 *Topic 1*

Besides the Personal Data Protection Act (PDPA), which of the following is a potential source of privacy protection for Singapore citizens?

A. Constitutional protections of personal information.

B. International agreements protecting privacy.

C. The tort of invasion of privacy.

D. Breach of confidence law.

Suggested Answer: *A*

Community vote distribution

Bhimesh 5 months, 2 weeks ago

Selected Answer: D

D- breach of confidence law.

upvoted 1 times

Bhimesh 5 months, 3 weeks ago

D- breach of confidence law.

Singapore provides very little legal protection to privacy outside the new PDPA. It has no explicit constitutional protections of privacy, and it is not a party to any enforceable international agreements protecting privacy. It is uncertain whether there is tort protection against harassment, but otherwise there is no tort of invasion of privacy. Some protection is provided by breach of confidence law.

upvoted 1 times

187b1e6 6 months, 2 weeks ago

should be D breach of confidence law

upvoted 2 times

Achatterjee 1 year, 2 months ago

Selected Answer: C

Invasion Of Privacy Elements And Its Legal Laws To Comply

upvoted 1 times

Question #9 *Topic 1*

Which of the following would NOT be exempt from Singapore's PDPA?

A. A government automobile registration website.

B. A private party room at a popular restaurant.

C. A documentary filmed at a rock concert.

D. A video from a store's dosed-circuit TV.

Suggested Answer: *D*

Community vote distribution

D (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: D

D. A video from a store's dosed-circuit TV.

upvoted 1 times

Question #10 *Topic 1*

SCENARIO – Please use the following to answer the next question:
Delilah is seeking employment in the marketing department of Good Mining Private Limited, an industry leader in drilling mines in Singapore. Delilah, while filling in the standard paper application form, is asked to provide details about emergency contacts, medical history, blood type and her insurance policy. These fields need to be filled in no matter which department Delilah applies to. The form also asks Delilah to expressly consent to the collection, use and disclosure of her personal data.
A week after submitting the form, Delilah is invited by Evan, the Director of Marketing at Good Mining, to coffee. Just before Delilah leaves, she gives her business card containing her current business contact information to Evan. Evan then uses the business card to add Delilah's details to Good Mining's business development database, which is kept on a local server. Good Mining uses the database to inform people about networking and client events that Good Mining organizes.
Why is it legal for Evan to add the information on Delilah's business card to the business development database?

A. Because Delilah "consented" to her business contact information being used by Good Mining by passing it to Evan voluntarily.

B. Because any business contact information can be freely used, collected or disclosed by Good Mining.

C. Because Good Mining does not export the information to a cloud vendor.

D. Because Delilah initiated the relationship with Good Mining.

Suggested Answer: *B*

Community vote distribution

B (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: B

B. Because any business contact information can be freely used, collected or disclosed by Good Mining.

upvoted 1 times

Question #11 *Topic 1*

SCENARIO – Please use the following to answer the next question:
Delilah is seeking employment in the marketing department of Good Mining Private Limited, an industry leader in drilling mines in Singapore. Delilah, while filling in the standard paper application form, is asked to provide details about emergency contacts, medical history, blood type and her insurance policy. These fields need to be filled in no matter which department Delilah applies to. The form also asks Delilah to expressly consent to the collection, use and disclosure of her personal data.
A week after submitting the form, Delilah is invited by Evan, the Director of Marketing at Good Mining, to coffee. Just before Delilah leaves, she gives her business card containing her current business contact information to Evan. Evan then uses the business card to add Delilah's details to Good Mining's business development database, which is kept on a local server. Good Mining uses the database to inform people about networking and client events that Good Mining organizes.
Why is Good Mining Private's standard form NOT compliant with Singapore's data protection law?

A. It is not available in an electronic format.

B. It does not contain the contact information for the HR manager.

C. It asks for Delilah's consent to use and disclose her personal data.

D. It asks for details that are not relevant to the job Delilah is applying for.

Suggested Answer: *D*

Community vote distribution

D (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: D

D. It asks for details that are not relevant to the job Delilah is applying for.

upvoted 1 times

Alizade 1 year, 6 months ago

Selected Answer: D

The reason why Good Mining Private's standard form is NOT compliant with Singapore's data protection law is option D, as it asks for details that are not relevant to the job Delilah is applying for. Singapore's Personal Data Protection Act (PDPA) requires that organizations only collect, use, and disclose personal data for purposes that are reasonable and relevant. Asking for information such as emergency contacts, medical history, blood type, and insurance policy is not necessary or relevant to Delilah's job application in the marketing department. Therefore, it is considered excessive collection of personal data, which is a violation of the PDPA. Additionally, the collection and use of Delilah's business card for purposes other than what was explicitly agreed to by Delilah, which was to contact her for coffee, may also be a violation of the PDPA.

upvoted 1 times

Question #12 *Topic 1*

Which of the following does Singapore's PDPC NOT have the power to do?

A. Order an organization to stop collecting personal data.

B. Order an organization to destroy collected personal data.

C. Order an organization to award compensation to a complainant.

D. Order an organization to pay a financial penalty to the government.

Suggested Answer: *D*

Community vote distribution

C (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: C

Enforcement of the Data Protection

If the PDPC finds that an organisation has breached any of the PDPA provisions, we will direct the organisation to take steps to ensure compliance such as:

Stop collecting, using or disclosing personal data in contravention of the Act;

Destroy personal data collected in contravention of the Act;

Provide access to or correct the personal data; and/or

Pay a financial penalty.

upvoted 1 times

Bhimesh 5 months, 2 weeks ago

It should however be noted that the Commission is not empowered to award damages

to a complainant

. As such, the Commission will generally prefer to take other measures (such as facilitation and alternative dispute resolution mechanisms like mediation) to encourage the parties to discuss the issues in a complaint and find a mutually acceptable resolution, which may include compensation.

upvoted 1 times

Bhimesh 5 months, 2 weeks ago

The Commission is not empowered to award damages or other relief noted above to a complainant, persons who suffer loss or damage as a result of a contravention of the PDPA may commence civil proceedings directly. In general, such persons may wish to obtain legal advice in relation to their claim and possible civil proceedings.

upvoted 1 times

187b1e6 6 months, 2 weeks ago

should be C - https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/enforcement-of-the-act

upvoted 2 times

Question #13 *Topic 1*

SCENARIO – Please use the following to answer the next question:
Singabank is a boutique bank in Singapore. After being notified during the hiring process, Singabank employees are subject to constant and thorough monitoring and tracking through CCTV cameras, computer monitoring software and keyboard loggers. Singabank does this to ensure its employees are complying with Singabank's data security policy. Bigbank is now considering acquiring Singabank's retail banking division. As part of its due diligence, Bigbank is seeking for Singabank to disclose to it all of its surveillance material on its employees, whether or not they are part of the retail banking division. Jimmy works in Singabank's investment banking division.
What would make Singabank's monitoring of its employees illegal?

A. If the employees did not explicitly consent to it.

B. If the bank's data security policy was being overhauled.

C. If the bank collected employees' sensitive personal information.

D. If the employees were not provided contact information to ask questions about the monitoring.

Suggested Answer: *A*

Community vote distribution

A (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: A

A. If the employees did not explicitly consent to it.

upvoted 1 times

Question #14 *Topic 1*

SCENARIO – Please use the following to answer the next question:
Singabank is a boutique bank in Singapore. After being notified during the hiring process, Singabank employees are subject to constant and thorough monitoring and tracking through CCTV cameras, computer monitoring software and keyboard loggers. Singabank does this to ensure its employees are complying with Singabank's data security policy. Bigbank is now considering acquiring Singabank's retail banking division. As part of its due diligence, Bigbank is seeking for Singabank to disclose to it all of its surveillance material on its employees, whether or not they are part of the retail banking division. Jimmy works in Singabank's investment banking division.
Assuming the monitoring was legal, can Singabank disclose Jimmy's personal data to Bigbank?

A. No, because Jimmy is not in the division that Bigbank seeks to acquire.

B. No, because the data was collected for the express purpose of complying with Singabank's privacy policies.

C. Yes, if Singabank informs Jimmy of the disclosure of his personal data before it occurs.

D. Yes, if Jimmy's personal data is necessary for Bigbank to determine whether to proceed with the acquisition.

Suggested Answer: *C*

Community vote distribution

D (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: D

D. Yes

upvoted 1 times

rhyst1921 5 months, 3 weeks ago

C would be correct IF Jimmy's consent was sought, however in this option C, it is incorrect because simply notification is insufficient.

upvoted 1 times

rhyst1921 5 months, 3 weeks ago

Selected Answer: D

D, as this would likely fall under the business asset transaction exception from consent obligation under the PDPA.

upvoted 1 times

187b1e6 6 months, 2 weeks ago

should be D

upvoted 1 times

Question #15 *Topic 1*

In which of the following cases would a Singaporean be prevented from accessing information about herself from an organization?

A. The information was collected in the previous 12 months.

B. The information is related to an individual's credit rating.

C. The cost of providing the information proved to be unreasonable.

D. Any personal information about others has been deleted from the document.

Suggested Answer: *B*

Community vote distribution

C (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: C

The exceptions specified in the Fifth Schedule include the following matters:
Organisations should note that they are not required to provide access if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interest or if the request is otherwise frivolous or vexatious.

j) any request —
i. that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests;
ii. if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interests;
upvoted 1 times

rhyst1921 5 months, 4 weeks ago

Selected Answer: C

Should be C
upvoted 1 times

Question #16 *Topic 1*

Which of the following principles of the OECD guidelines and Council of European Convention principles does Singapore's PDPA incorporate?

A. Disclosures to third parties included in access requests.

B. Additional protections for sensitive personal data.

C. The ability to opt-out from direct marketing.

D. The right of deletion of data on request.

Suggested Answer: *C*

Community vote distribution

C (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: C

C. The ability to opt-out from direct marketing.

upvoted 1 times

rhyst1921 5 months, 3 weeks ago

Selected Answer: C

A is wrong as this principle is not explicitly mentioned in the OECD guidelines or the Council of European Convention principles. B is wrong as there is no concept of sensitive personal data under the PDPA. D is also wrong as there is no right of deletion under the PDPA.

C is correct as under the PDPA, the data subjects have the right to withdrawal of consent from direct marketing. Both the OECD guidelines and the Council of European Convention principles emphasize the importance of individuals having the ability to opt-out from direct marketing.

upvoted 1 times

Question #17 *Topic 1*

SCENARIO – Please use the following to answer the next question:
B-Star Limited is a Singapore based construction company with many foreign construction workers. B-Star's HR team maintains two databases. One (the "simple database") contains basic details from a standard in-processing form such as name, local address and mobile number. The other database (the "sensitive database") contains information collected by the HR Department as part of Annual Review Interviews. With the workers' cooperation, this database has expanded to include far-reaching sensitive information such as medical history, religious beliefs, ethnicity and educational levels of immediate family members. Carl left B-Star's employment yesterday, and has flown back home, rendering him unreachable. Today B-Star, without Carl's consent, wants to conduct research using Carl's medical records in the sensitive database.
Can B-Star legally conduct this research using Carl's medical data?

A. Yes, because Carl gave his consent for his sensitive personal data to be collected during his employment.

B. No, an organization is not allowed to use sensitive personal data without an individual's consent unless absolutely necessary.

C. No, because the research is taking place after Carl has left B-Star's employment.

D. Yes, if the research is deemed to be in the public interest.

Suggested Answer: *B*

Community vote distribution

D (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: D

'research'

upvoted 1 times

rhyst1921 5 months, 4 weeks ago

should be D, this is an exemption provided under Schedule 2 of the PDPA

upvoted 1 times

Question #18 *Topic 1*

A Singapore employer can do all of the following without obtaining an employee's consent EXCEPT?

A. Share an employee's personal data with a company that provides financial planning.

B. Disclose personal health data to a public agency during a health crisis.

C. Use computer monitoring software on an employee's computers.

D. Use closed-circuit television surveillance in the workplace.

Suggested Answer: *A*

Community vote distribution

A (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: A

A. Share an employee's personal data with a company that provides financial planning.

upvoted 1 times

Question #19 *Topic 1*

Which control is NOT included in the requirements established by the Monetary Authority of Singapore (MAS) for financial institutions in order to deter money-laundering and financial aid to terrorism (AML/CFT)?

A. Identifying and knowing customers.

B. Sharing personal information with the PDPC.

C. Conducting regular reviews of customer accounts.

D. Monitoring and reporting suspicious financial transactions.

Suggested Answer: *A*

Community vote distribution

B (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: B

The AML/CFT requirements for banks:

Risk assessment and risk mitigation.
Customer due diligence.
Reliance on third parties.
Correspondent banking and wire transfers.
Record keeping.
Suspicious transaction reporting.
Internal policies, compliance, audit and training.

At the regulatory level, the PDPC, MAS and CSA can work closely and collaborate with each other to enhanced the data protection
1.6 In this respect, we recommend:
(a) Collaborative reporting between FIs and MAS, CSA and PDPC (collectively, the "regulatory agencies"), where notifying MAS and/or PDPC in the event of a data breach will suffice.
(b) Collaborative investigating between FIs and the regulatory agencies, where only MAS and/or PDPC will investigate should the need arise.
(c) Greater coordination between the regulatory agencies.

upvoted 1 times

rhyst1921 5 months, 4 weeks ago

Selected Answer: B

MAS does not require sharing of personal information with the PDPC. Indentifying and knowing customers, on the other had, is part of KYC requirements that is integral to PMLTF.

upvoted 1 times

Question #20 *Topic 1*

All of the following are guidelines the PDPC gives about anonymised data EXCEPT?

A. Anonymised data is not personal data.

B. Any data that has been anonymised bears the same risks for re-identification.

C. Data that has been anonymised satisfies the "cease to retain" requirement of Section 25.

D. Organizations should consider the risk of re-identification if it intends to publish or disclose anonymised data.

Suggested Answer: *C*

Community vote distribution

C (67%) D (33%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: C

C. Data that has been anonymised satisfies the "cease to retain" requirement of Section 25.

upvoted 1 times

rhyst1921 5 months, 3 weeks ago

Not B because this statement is generally true. Even though data has been anonymised, there's always a risk, albeit reduced, of re-identification, especially with advancements in technology.

upvoted 1 times

rhyst1921 5 months, 3 weeks ago

Selected Answer: C

(Correction) Anonymising data doesn't necessarily satisfy the requirement to cease retention. Ceasing retention typically refers to deleting or securely disposing of personal data once it's no longer needed for its original purpose.

upvoted 1 times

rhyst1921 5 months, 4 weeks ago

Selected Answer: D

Should be D. The 'cease to retain', i.e. retention, requirement under Section 25 of the PDPA is met if the personal data is anonymised. An organisation will be considered to have ceased to retain personal data when it no longer has the means to associate the personal data with particular individuals – i.e. the personal data has been anonymised.

upvoted 1 times

Question #21 *Topic 1*

Under what circumstances are smart identity cards required of Hong Kong citizens?

A. When opening bank accounts.

B. When using public transit systems.

C. When seeking government services.

D. When making substantial purchases.

Suggested Answer: *C*

Community vote distribution

A (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: A

A. When opening bank accounts.

upvoted 1 times

Achatterjee 1 year ago

Selected Answer: A

A is correct

upvoted 1 times

Question #22 *Topic 1*

Hong Kong's Personal Data (Privacy) Ordinance (PDPO) was primarily inspired by which of the following?

A. Asia's APEC Privacy Framework.

B. Macau's Personal Data Protection Act.

C. South Korea's Public Agency Data Protection Act.

D. Europe's Data Protection Directive (Directive 95/46/EC).

Suggested Answer: *D*

Community vote distribution

D (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: D

Origins of, and influences on, the Ordinance

The Ordinance's enactment was not prompted by any significant public demands or major controversy, but was led by the then colonial administration, influenced by local elite opinion. It was a positive and not a reactive process, influenced by European developments and their potential effect on trade with Hong Kong. The history of the Ordinance's development shows that the Hong Kong government was concerned about possible limits on personal data flows from Europe as early as the 1981 Council of Europe Data Protection Convention,

BUT heightening in the early 1990s as the European Union (EU) Data Protection Directive developed. From 1989 the HKLRC was given a very broad reference on privacy protection, and following public consultations published recommendations for data protection legislation, the majority of which were embodied in the 1995 Ordinance.

upvoted 1 times

Question #23 *Topic 1*

Hong Kong's definition of a data user in the original PDPO applies to all of the following EXCEPT?

A. Trust corporations.

B. Third-party processors.

C. Private sector organizations.

D. Limited liability partnerships.

Suggested Answer: *B*

Community vote distribution

B (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: B

Data User is a person who, either alone or jointly with other persons, controls the collection, holding, processing or use of personal data.

Data user (Controller) Data Intermediary (Vendor , Data processor)
The Data Intermediary is referred to differently depending upon the country or jurisdiction. In Singapore, it is data intermediary.

In EU – the data processor,
And in the United States / India – a data processor is typically referred to as a vendor, service provider or a third-party service provider
upvoted 1 times

Bhimesh 5 months, 2 weeks ago

A party who is only processing the data as agent for another person (a processor) is not a data user.
upvoted 1 times

Question #24 *Topic 1*

In what way are Hong Kong citizens protected from direct marketing in ways that India and Singapore citizens are not?

A. Subscribers must have explicitly indicated that they did not object to their data being collected and used for marketing purposes.

B. Subscribers can opt out of the use of their data for marketing purposes after collection by withdrawing consent.

C. Data subjects must be notified on a website if their data is being used for marketing purposes.

D. Data subjects are protected from the secondary use of personal data for marketing purposes.

Suggested Answer: *A*

Community vote distribution

A (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: A

A. Subscribers must have explicitly indicated that they did not object to their data being collected and used for marketing purposes

upvoted 1 times

Question #25 *Topic 1*

SCENARIO – Please use the following to answer the next question:
Zoe is the new Compliance Manager for the Star Hotel Group, which has five hotels across Hong Kong and China. On her first day, she does an inspection of the largest property, StarOne. She starts with the hotel reception desk. Zoe sees the front desk assistant logging in to a database as he is checking in a guest. The hotel manager, Bernard, tells her that all guest data, including passport numbers, credit card numbers, home address, mobile number and other information associated with a guest's stay is held in a database. Bernard tells her not to worry about the security of the database because it is operated for Star Hotels by a local service provider called HackProof, who therefore are responsible for all the guest data.
Zoe notices what looks like a CCTV camera in the corner of the reception area. Bernard says they record all activity in the lobby. In fact, last Tuesday he had received a data access request from a lawyer requesting a copy of footage of all lobby activity for the preceding month. The lawyer's covering letter said that his client has never visited the hotel herself, but is investigating whether her husband has been doing so without her knowledge.
Zoe and Bernard head up to the hotel spa. The spa is independently owned by a company called Relax Ltd. Bernard explains that Relax Ltd is a small company and, as they don't have their own database, they transfer data about the spa guests to StarOne staff so that they can upload the data into the HackProof system. Relax Ltd staff can then login and review their guest data as needed.
Zoe asks more about the HackProof system. Bernard tells her that the server for the Hong Kong hotels is in Hong Kong, but there is a server in Shenzhen that has a copy of all the Hong Kong hotel data and supports the properties in China. The data is in China for back up purposes and also is accessible by staff in the China hotels so they can better service guests who visit their hotels in both territories.
How should Bernard respond to the lawyer's request for the CCTV footage?

A. Decline to turn over the footage as it is not a valid data access request.

B. Provide a copy of the footage within 40 days as it is a data access request.

C. Provide a copy of the footage to the lawyer under the exemption for legal professional privilege.

D. Decline to turn over the footage as there is no basis for it to be disclosed under the exemption for prevention or detection of crime.

Suggested Answer: *D*

Community vote distribution

D (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: D

Exemptions
While data privacy is an important right, the interests protected under PDPO have to be balanced against other important rights or public interest. PDPO provides a number of exemptions from some compliance requirements under particular circumstances. Examples include crime prevention or prosecution, security and defence, statistics and research, news activity, protecting a data subject's health etc. There is also an exemption if the use of personal data is required or authorised by law or court order or is required for exercising or defending legal rights in Hong Kong.

Prevention or detection of crime

According to section 58 of the Ordinance, personal data held for the purpose of prevention or detection of a crime may be exempt from the provisions in respect of data-access requests (DPP 6 and section 18(1)(b) of the Ordinance) and restrictions on the use of personal data (DPP 3).
upvoted 1 times

Question #26 *Topic 1*

SCENARIO – Please use the following to answer the next question:
Zoe is the new Compliance Manager for the Star Hotel Group, which has five hotels across Hong Kong and China. On her first day, she does an inspection of the largest property, StarOne. She starts with the hotel reception desk. Zoe sees the front desk assistant logging in to a database as he is checking in a guest. The hotel manager, Bernard, tells her that all guest data, including passport numbers, credit card numbers, home address, mobile number and other information associated with a guest's stay is held in a database. Bernard tells her not to worry about the security of the database because it is operated for Star Hotels by a local service provider called HackProof, who therefore are responsible for all the guest data.
Zoe notices what looks like a CCTV camera in the corner of the reception area. Bernard says they record all activity in the lobby. In fact, last Tuesday he had received a data access request from a lawyer requesting a copy of footage of all lobby activity for the preceding month. The lawyer's covering letter said that his client has never visited the hotel herself, but is investigating whether her husband has been doing so without her knowledge.
Zoe and Bernard head up to the hotel spa. The spa is independently owned by a company called Relax Ltd. Bernard explains that Relax Ltd is a small company and, as they don't have their own database, they transfer data about the spa guests to StarOne staff so that they can upload the data into the HackProof system. Relax Ltd staff can then login and review their guest data as needed.
Zoe asks more about the HackProof system. Bernard tells her that the server for the Hong Kong hotels is in Hong Kong, but there is a server in Shenzhen that has a copy of all the Hong Kong hotel data and supports the properties in China. The data is in China for back up purposes and also is accessible by staff in the China hotels so they can better service guests who visit their hotels in both territories.
HackProof reports to Zoe that a copy of the entire guest database has been exfiltrated by a hacker.
What is Zoe's best course of action?

A. Zoe must immediately notify all guests, the police and the Privacy Commissioner of the breach.

B. Zoe does not need to do anything as there is no mandatory breach notification requirement in Hong Kong.

C. Zoe must report the breach to the Privacy Commissioner and make an action plan together with the Commissioner.

D. Zoe should consider if there is a real risk of harm to the guests and take appropriate action based on her assessment.

Suggested Answer: *D*

Community vote distribution

D (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: D

HANDLING DATA BREACHES

The following steps are recommended when handling a data breach.

Step 1: Immediate gathering of essential information
Step 2: Containing the data breach
Step 3: Assessing the risk of harm
Step 4: Considering giving data breach notifications
Step 5: Documenting the breach
Assessing the risk of harm
Once all essential information has been gathered, the data users should then ensure that they understand the risks of harm that may be caused to the affected individuals, so that they can take steps to limit the impact.
upvoted 1 times

Bhimesh 5 months, 2 weeks ago

Notifying the data subjects is next if the breach has serious problems like
....The possible harm caused by a
data breach may include:
• Threats to personal safety
• Identity theft
• Financial loss
• Humiliation or loss of dignity, damage to

reputation or relationships

- Loss of business or employment opportunities

upvoted 1 times

Question #27 *Topic 1*

SCENARIO – Please use the following to answer the next question:
Zoe is the new Compliance Manager for the Star Hotel Group, which has five hotels across Hong Kong and China. On her first day, she does an inspection of the largest property, StarOne. She starts with the hotel reception desk. Zoe sees the front desk assistant logging in to a database as he is checking in a guest. The hotel manager, Bernard, tells her that all guest data, including passport numbers, credit card numbers, home address, mobile number and other information associated with a guest's stay is held in a database. Bernard tells her not to worry about the security of the database because it is operated for Star Hotels by a local service provider called HackProof, who therefore are responsible for all the guest data.
Zoe notices what looks like a CCTV camera in the corner of the reception area. Bernard says they record all activity in the lobby. In fact, last Tuesday he had received a data access request from a lawyer requesting a copy of footage of all lobby activity for the preceding month. The lawyer's covering letter said that his client has never visited the hotel herself, but is investigating whether her husband has been doing so without her knowledge.
Zoe and Bernard head up to the hotel spa. The spa is independently owned by a company called Relax Ltd. Bernard explains that Relax Ltd is a small company and, as they don't have their own database, they transfer data about the spa guests to StarOne staff so that they can upload the data into the HackProof system. Relax Ltd staff can then login and review their guest data as needed.
Zoe asks more about the HackProof system. Bernard tells her that the server for the Hong Kong hotels is in Hong Kong, but there is a server in Shenzhen that has a copy of all the Hong Kong hotel data and supports the properties in China. The data is in China for back up purposes and also is accessible by staff in the China hotels so they can better service guests who visit their hotels in both territories.
Assuming that Section 33 is in force, which of the following would NOT help Zoe to facilitate the cross-border transfer from Hong Kong to China?

A. Consent of the guest in writing to the transfer.

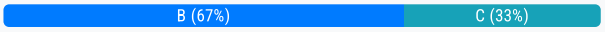
B. Amending StarOne's privacy policy to refer to the transfer.

C. Putting in place Model Clauses between the relevant entities.

D. China being included as a "White List" country for data transfer.

Suggested Answer: *A*

Community vote distribution



Bhimesh 5 months, 2 weeks ago

Selected Answer: B

CORRECTION - answer 'B'

upvoted 1 times

Bhimesh 5 months, 2 weeks ago

Selected Answer: C

Section 2: Exceptions to Cross border transfer restrictions under section 33(2)
Option A : Section 33(2)(c) data subject's consent in writing to the transfer
Option C: Model Clauses which may be adapted and/or included in a data
transfer agreement by parties who wish to transfer personal data outside Hong Kong in accordance with section 33(2)(f) of the Personal Data (Privacy) Ordinance (the "Ordinance").
Option D: Section 33(2)(a) White List jurisdictions as specified by the Commissioner in the Gazette

upvoted 1 times

rhyst1921 5 months, 4 weeks ago

Selected Answer: B

Should be B. A is permitted under section 33(2)(c), D is permitted under section 33(2)(a), and putting in the model clauses is permitted under section 33(2)(f).

upvoted 1 times

Question #28 *Topic 1*

SCENARIO – Please use the following to answer the next question:
Zoe is the new Compliance Manager for the Star Hotel Group, which has five hotels across Hong Kong and China. On her first day, she does an inspection of the largest property, StarOne. She starts with the hotel reception desk. Zoe sees the front desk assistant logging in to a database as he is checking in a guest. The hotel manager, Bernard, tells her that all guest data, including passport numbers, credit card numbers, home address, mobile number and other information associated with a guest's stay is held in a database. Bernard tells her not to worry about the security of the database because it is operated for Star Hotels by a local service provider called HackProof, who therefore are responsible for all the guest data.
Zoe notices what looks like a CCTV camera in the corner of the reception area. Bernard says they record all activity in the lobby. In fact, last Tuesday he had received a data access request from a lawyer requesting a copy of footage of all lobby activity for the preceding month. The lawyer's covering letter said that his client has never visited the hotel herself, but is investigating whether her husband has been doing so without her knowledge.
Zoe and Bernard head up to the hotel spa. The spa is independently owned by a company called Relax Ltd. Bernard explains that Relax Ltd is a small company and, as they don't have their own database, they transfer data about the spa guests to StarOne staff so that they can upload the data into the HackProof system. Relax Ltd staff can then login and review their guest data as needed.
Zoe asks more about the HackProof system. Bernard tells her that the server for the Hong Kong hotels is in Hong Kong, but there is a server in Shenzhen that has a copy of all the Hong Kong hotel data and supports the properties in China. The data is in China for back up purposes and also is accessible by staff in the China hotels so they can better service guests who visit their hotels in both territories.
Members of Relax Ltd's staff are concerned about the data sharing with StarOne.
How should Zoe respond to their concerns?

A. Inform the staff that Relax Ltd can transfer the data to StarOne given they are in the same premises and guests would reasonably expect that.

B. Inform the staff that Relax Ltd should not transfer the data to StarOne without a privacy notice identifying StarOne as a class of transferee.

C. Inform the staff that Relax Ltd should not transfer the data to StarOne without the guest's opt-in consent to do so.

D. Inform the staff that Relax Ltd can transfer the data as Section 33 is not in force.

Suggested Answer: *C*

Bhimesh 5 months, 2 weeks ago
Yup, C. Inform the staff that Relax Ltd should not transfer the data to StarOne without the guest's opt-in consent to do so.
upvoted 1 times

Question #29 *Topic 1*

Increases in which of the following were a major reason for the enactment of Hong Kong's Amendment Ordinance in 2012?

A. Direct marketing practices.

B. Law enforcement requests.

C. Biometric authentication.

D. Data breach reports.

Suggested Answer: *A*

Community vote distribution

A (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: A

Should be A. Direct marketing practices.

upvoted 1 times

Question #30 *Topic 1*

The "due diligence" exemption in Hong Kong's PDPO was meant to apply to?

A. Third-party data processors located in foreign countries.

B. Companies researching the viability of business mergers.

C. Service providers hosting customer information in the cloud.

D. Direct marketers acting in the best interest of their company.

Suggested Answer: *A*

Community vote distribution

B (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: B

4.15 The question may arise as to whether the requirements under this Part applies to the situation where personal data is provided to another person due to a merger or business amalgamation involving a sale of business or shares. The short answer is that the requirements under this Part do not apply if the personal data provided is not for use in direct marketing.

Otherwise, consent has to be obtained from the data subject. Data users should be mindful that if the provision is for use in direct marketing under the guise of a merger or acquisition, they are still liable under the Ordinance.

upvoted 1 times

Rongchen 1 year, 9 months ago

Should be B

upvoted 3 times

Question #31 *Topic 1*

Hong Kong's New Guidance on Direct Marketing clarified that direct marketing rules under the new regime do NOT apply if what condition exists?

A. The data subject's personal data is collected from public registers or third parties.

B. The products or services are being offered by the organization's parent company.

C. The data subject has already given consent for other services offered by the company.

D. The products or services are being offered for the exclusive use of an individual's organization.

Suggested Answer: *C*

Community vote distribution

C (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: C

C. The data subject has already given consent for other services offered by the company.

upvoted 1 times

Question #32 *Topic 1*

SCENARIO – Please use the following to answer the next question:
Fitness For Everyone ("FFE") is a gym on Hong Kong Island that is affiliated with a network of gyms throughout Southeast Asia. When prospective members of the gym stop in, call in or submit an inquiry online, they are invited for a free trial session. At first, the gym asks prospective clients only for basic information: a full name, contact number, age and their Hong Kong ID number, so that FFE's senior trainer Kelvin can reach them to arrange their first appointment.
One day, a potential customer named Stephen took a tour of the gym with Kelvin and then decided to join FFE for six months. Kelvin pulled out a registration form and explained FFE's policies, placing a circle next to the part that read "FEE and affiliated third parties" may market new products and services using the contact information provided on the form to Stephen "for the duration of his membership." Stephen asked if he could opt-out of the marketing communications. Kelvin shrugged and said that it was a standard part of the contract and that most gyms have it, but that even so Kelvin's manager wanted the item circled on all forms. Stephen agreed, signed the registration form at the bottom of the page, and provided his credit card details for a monthly gym fee. He also exchanged instant messenger/cell details with Kelvin so that they could communicate about personal training sessions scheduled to start the following week.
After attending the gym consistently for six months, Stephen's employer transferred him to another part of the Island, so he did not renew his FFE membership.
One year later, Stephen started to receive numerous text messages each day from unknown numbers, most marketing gym or weight loss products.
Suspecting that FFE shared his information widely, he contacted his old FFE branch and asked reception if they still had his information on file. They did, but offered to delete it if he wished. He was told FFE's process to purge his information from all the affiliated systems might take 8 to 12 weeks. FFE also informed him that Kelvin was no longer employed by FFE and had recently started working for a competitor. FFE believed that Kelvin may have shared the mobile contact details of his clients with the new gym, and apologized for this inconvenience.
Assuming that Kelvin received a commission for sharing his former client list with the new employer, and the new employer used Stephen's data to engage in direct marketing to Stephen, which of the following penalties could Kelvin face under Part VI A of the Ordinance?

A. No penalty, as FFE and the new employer are the responsible parties.

B. Violation of the terms of his employment agreement.

C. A maximum $500,000 HKD fine.

D. Up to five years imprisonment.

Suggested Answer: *B*

Community vote distribution

D (100%)

rhyst1921 5 months, 4 weeks ago

Selected Answer: D

Up to 5 yrs imprisonment or fine of HKD1mil max for breach of direct marketing rules for gain. Not for gain - max 3 yrs imprisonment or HKD500K fine.

upvoted 1 times

Achatterjee 1 year ago

Selected Answer: D

D. Also mentioned in Part VI

upvoted 1 times

Question #33 *Topic 1*

SCENARIO – Please use the following to answer the next question:
Fitness For Everyone ("FFE") is a gym on Hong Kong Island that is affiliated with a network of gyms throughout Southeast Asia. When prospective members of the gym stop in, call in or submit an inquiry online, they are invited for a free trial session. At first, the gym asks prospective clients only for basic information: a full name, contact number, age and their Hong Kong ID number, so that FFE's senior trainer Kelvin can reach them to arrange their first appointment.
One day, a potential customer named Stephen took a tour of the gym with Kelvin and then decided to join FFE for six months. Kelvin pulled out a registration form and explained FFE's policies, placing a circle next to the part that read "FEE and affiliated third parties" may market new products and services using the contact information provided on the form to Stephen "for the duration of his membership." Stephen asked if he could opt-out of the marketing communications. Kelvin shrugged and said that it was a standard part of the contract and that most gyms have it, but that even so Kelvin's manager wanted the item circled on all forms. Stephen agreed, signed the registration form at the bottom of the page, and provided his credit card details for a monthly gym fee. He also exchanged instant messenger/cell details with Kelvin so that they could communicate about personal training sessions scheduled to start the following week.
After attending the gym consistently for six months, Stephen's employer transferred him to another part of the Island, so he did not renew his FFE membership.
One year later, Stephen started to receive numerous text messages each day from unknown numbers, most marketing gym or weight loss products.
Suspecting that FFE shared his information widely, he contacted his old FFE branch and asked reception if they still had his information on file. They did, but offered to delete it if he wished. He was told FFE's process to purge his information from all the affiliated systems might take 8 to 12 weeks. FFE also informed him that Kelvin was no longer employed by FFE and had recently started working for a competitor. FFE believed that Kelvin may have shared the mobile contact details of his clients with the new gym, and apologized for this inconvenience.
Which of the following FFE data retention policies would be permitted under Section 26 of the Personal Data (Privacy) Ordinance and Hong Kong Data Protection Principle 2 regarding accuracy and retention?

A. Retain the data of members who have been suspended for non-payment, in the event that the data is needed to seek compensation in a court of law.

B. Retain all member data and documents in original form for two years after account termination, to better inform marketing efforts focused on re-activating accounts of former customers.

C. Retain an anonymous data set after account termination indicating dates of membership, age, and other statistical data, to be included in aggregate reports about gym membership trends.

D. Retain copies of files of customers who utilized personal trainer services for six months after account termination, to allow trainers to respond to inquiries from personal physicians about training-related injuries.

Suggested Answer: *C*

Bhimesh 5 months, 3 weeks ago
DPP2 Accuracy and Duration of Retention
DPP2 requires data users to take all practicable steps to ensure that personal data is accurate and is not keptlonger than is necessary for the fulfillment of the purpose for which the data is used. If you engage a dataprocessor for handling personal data of other persons, you should adopt contractual or other means to ensure thatthe data processor comply with the mentioned retention requirement.
Section 26 of PDPO requires data users to take all practicable steps to erase personal data that is no longerrequired for the purpose for which the data is used, unless erasure is prohibited by law or is not in the publicinterest. Section 26 could be engaged when a data user fails to respond to a complaint or request from a datasubject for erasure of personal data. This situation attracts a heavier criminal gravity than just keeping the datalonger than is necessary under DPP2. Contravention of the requirement under section 26 is an offence,punishable by a fine of up to HK$10,000
upvoted 1 times

Question #34 *Topic 1*

SCENARIO – Please use the following to answer the next question:
Fitness For Everyone ("FFE") is a gym on Hong Kong Island that is affiliated with a network of gyms throughout Southeast Asia. When prospective members of the gym stop in, call in or submit an inquiry online, they are invited for a free trial session. At first, the gym asks prospective clients only for basic information: a full name, contact number, age and their Hong Kong ID number, so that FFE's senior trainer Kelvin can reach them to arrange their first appointment.
One day, a potential customer named Stephen took a tour of the gym with Kelvin and then decided to join FFE for six months. Kelvin pulled out a registration form and explained FFE's policies, placing a circle next to the part that read "FEE and affiliated third parties" may market new products and services using the contact information provided on the form to Stephen "for the duration of his membership." Stephen asked if he could opt-out of the marketing communications. Kelvin shrugged and said that it was a standard part of the contract and that most gyms have it, but that even so Kelvin's manager wanted the item circled on all forms. Stephen agreed, signed the registration form at the bottom of the page, and provided his credit card details for a monthly gym fee. He also exchanged instant messenger/cell details with Kelvin so that they could communicate about personal training sessions scheduled to start the following week.
After attending the gym consistently for six months, Stephen's employer transferred him to another part of the Island, so he did not renew his FFE membership.
One year later, Stephen started to receive numerous text messages each day from unknown numbers, most marketing gym or weight loss products.
Suspecting that FFE shared his information widely, he contacted his old FFE branch and asked reception if they still had his information on file. They did, but offered to delete it if he wished. He was told FFE's process to purge his information from all the affiliated systems might take 8 to 12 weeks. FFE also informed him that Kelvin was no longer employed by FFE and had recently started working for a competitor. FFE believed that Kelvin may have shared the mobile contact details of his clients with the new gym, and apologized for this inconvenience.
Which of the following practices would likely violate Hong Kong's Data Protection Principle 1 regarding data collection?

A. FFE's collection of full name from prospective clients.

B. FFE affiliates' receipt of Stephen's contact information.

C. FFE's collection of age and HKID from prospective clients.

D. FFE's collection of Stephen's messenger cell details through Kelvin.

Suggested Answer: *D*

Community vote distribution

C (100%)

Bhimesh 5 months, 3 weeks ago

Answer C - - DP1 - Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user.
All practicable steps shall be taken to notify the data subjects of the purpose of data collection, and the classes of persons to whom the data may be transferred
DP1 - Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user.
All practicable steps shall be taken to notify the data subjects of the purpose of data collection, and the classes of persons to whom the data may be transferred

the option D is neccessary , hence wrong

upvoted 1 times

rhyst1921 5 months, 4 weeks ago

Selected Answer: C

Should be C, as collection of age and HKID number is excessive and not necessary.

upvoted 1 times

Question #35 *Topic 1*

SCENARIO – Please use the following to answer the next question:
Fitness For Everyone ("FFE") is a gym on Hong Kong Island that is affiliated with a network of gyms throughout Southeast Asia. When prospective members of the gym stop in, call in or submit an inquiry online, they are invited for a free trial session. At first, the gym asks prospective clients only for basic information: a full name, contact number, age and their Hong Kong ID number, so that FFE's senior trainer Kelvin can reach them to arrange their first appointment.
One day, a potential customer named Stephen took a tour of the gym with Kelvin and then decided to join FFE for six months. Kelvin pulled out a registration form and explained FFE's policies, placing a circle next to the part that read "FEE and affiliated third parties" may market new products and services using the contact information provided on the form to Stephen "for the duration of his membership." Stephen asked if he could opt-out of the marketing communications. Kelvin shrugged and said that it was a standard part of the contract and that most gyms have it, but that even so Kelvin's manager wanted the item circled on all forms. Stephen agreed, signed the registration form at the bottom of the page, and provided his credit card details for a monthly gym fee. He also exchanged instant messenger/cell details with Kelvin so that they could communicate about personal training sessions scheduled to start the following week.
After attending the gym consistently for six months, Stephen's employer transferred him to another part of the Island, so he did not renew his FFE membership.
One year later, Stephen started to receive numerous text messages each day from unknown numbers, most marketing gym or weight loss products.
Suspecting that FFE shared his information widely, he contacted his old FFE branch and asked reception if they still had his information on file. They did, but offered to delete it if he wished. He was told FFE's process to purge his information from all the affiliated systems might take 8 to 12 weeks. FFE also informed him that Kelvin was no longer employed by FFE and had recently started working for a competitor. FFE believed that Kelvin may have shared the mobile contact details of his clients with the new gym, and apologized for this inconvenience.
Which of the following types of text messages are permissible, regardless of Stephen's withdrawal of consent?

A. From the FFE retention department, offering a special discount for reactivating membership.

B. From health care services provided by Hong Kong's Hospital Authority or Department of Health.

C. From an FFE affiliate that provides a mechanism to opt out of further communications by reply-texting "OO."

D. From an FFE affiliate in the region Stephen was transferred to, offering services similar to those he purchased previously.

Suggested Answer: *C*

Community vote distribution

B (100%)

Bhimesh 5 months, 3 weeks ago

Selected Answer: B

Division 2—Use of Personal Data in Direct Marketing
35B. Application
This Division does not apply in relation to the offering, or advertising of the availability, of—
(a) social services run, subvented or subsidized by the Social Welfare Department;
(b) health care services provided by the Hospital Authority or Department of Health; or
(c) any other social or health care services which, if not provided, would be likely to cause serious harm to the physical or mental health of—
(i) the individual to whom the services are intended to be provided; or
(ii) any other individual.
upvoted 1 times

Bhimesh 5 months, 2 weeks ago

DPP3 Use of Data
DPP3 prohibits the use of personal data for any new purpose which is not or is unrelated to the original purpose when collecting the data, unless with the data subject's express and voluntary consent. A data subject can withdraw his/her consent previously given by written notice.

Regarding restrictions on use of personal data, Part 6A of the PDPO further requires that data users must obtain informed consent before using a data subject's personal data for direct marketing or transferring the data to a third party for direct marketing. The consent must be an explicit indication by the data subject and broadly covers an indication of no objection. In other words, silence cannot constitute consent.

upvoted 1 times

Question #36 *Topic 1*

In Hong Kong's revised Breach Guidance Note of 2015, what course of action did the Commissioner recommend that companies take immediately after experiencing a breach?

A. Proceed under the assumption that the breach is a threat to personal safety.

B. Enlist the aid of law enforcement to determine the cause of the breach.

C. Quickly issue a notification to the data subjects affected by the breach.

D. Immediately gather essential information in relation to the breach.

Suggested Answer: *B*

Community vote distribution

D (100%)

rhyst1921 5 months, 4 weeks ago

Selected Answer: D

Should be D: The commissioner recommends the following action plan:
Step 1: Immediately gather essential info relating to breach
Step 2: Contact interested parties and adopt measures to contain breach
Step 3: Assess the risk of harm
Step 4: Consider giving a data breach notification

upvoted 1 times

Rongchen 1 year, 9 months ago

Should be D

upvoted 2 times

Question #37 *Topic 1*

How was the Supreme Court's ruling in the Maneka Gandhi v Union of India case significant to Indian law?

A. It expanded the interpretation of right to life under Article 21 of the Constitution.

B. It established that privacy is a fundamental right granted by the Constitution under Article 21.

C. It upheld that the impounding of passports for "public interest" is allowable under Section 10(3)(c) of the Passports Act.

D. It ruled that under Article 32 of the Constitution individuals may file writ petitions when they feel their rights were violated.

Suggested Answer: *D*

Community vote distribution

A (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: A

The decision held by the Supreme Court has been a guiding light in understanding the aspects of fundamental rights mentioned part-iii of the Indian Constitution. This case deals with the principles of natural justice enshrined under Article 14 and 21 of the Indian Constitution.

Before this case article 21 only deals with assuring the right to life and personal liberty against the arbitrary actions of the executive but after the judgment of this case the scope of article 21 has been expanded and it take actions against the legislative also for the violation of fundamental rights mentioned under article 21.

The ruling of Maneka Gandhi case was handed down by the seven judge bench of the The Maneka Gandhi case is considered as the land mark case in the history of Indian Legal system because this case has widened the scope of Article 21 of the Indian constitution which provides the provision for protection of life and personal liberty

upvoted 1 times

rhyst1921 5 months, 4 weeks ago

Selected Answer: A

Should be A. This case became a landmark judgment for highlighting the importance of the right to life as an expansive right.

upvoted 1 times

Achatterjee 1 year ago

Selected Answer: A

It is A. It expanded

upvoted 1 times

Question #38 *Topic 1*

Which of the following entities do NOT fall under India's Right to Information Act of 2005?

A. High courts.

B. State legislatures.

C. Law enforcement agencies.

D. National Security Guard.

Suggested Answer: *D*

Community vote distribution

D (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: D

In the Central Act, section 8(1) lists all of the exemptions.

• National Security or Sovereignty: As explained above, there is some information, which relates to India's national security, which could genuinely cause harm if it was released to the public. For example, information published during a conflict, detailing the number of soldiers defending a boundary, where they were positioned or their strategic plans. However, it would not be appropriate to use this exemption simply to keep a contract for the purchase of an air force fighter jet secret. This is common commercial information which should be made public to reduce the likelihood of corruption tainting the procurement process, and should not be withheld simply because it relates to defence.

upvoted 1 times

Bhimesh 5 months, 2 weeks ago

The 'right to information' provided by the 2005 national legislation has a broad scope, covering 'information held by or under the control of any Public Authority'. 'Public authority' includes any body established under the Constitution, or Centre or state law, or under delegated legislation, and includes bodies owned or controlled by government or directly or indirectly substantially Financed by government (even if they are NGOs).

The reach of the legislation is therefore to all tiers of government and somewhat beyond that.

In 2004 India's Supreme Court conclusively interpreted article 19(1)(a) of the Constitution of India to impliedly include the right to information in the constitutional guarantees of freedom of speech and expression (People's Union for Civil Liberties v Union of India),

Five years before a similar conclusion was reached in Europe. National legislation was then enacted by the Centre as the Right to Information Act 2005 (RITA).

upvoted 1 times

Bhimesh 5 months, 2 weeks ago

It is extremely positive that the Central Act makes all of the exemptions contained in section 8(1) subject to a "Public Interest Override" (see section 8(2) of the Central Act). What this means is that even where requested information is covered by an exemption, the information should still be disclosed to the applicant if the public interest in the specific case requires it.

upvoted 1 times

rhyst1921 5 months, 4 weeks ago

Selected Answer: D

The NSG is a special forces unit under the Ministry of Home Affairs, and it may fall under the category of security and intelligence agencies which are generally exempt from the RTI Act, particularly when the information concerns matters of national security.

upvoted 1 times

Question #39 *Topic 1*

In India, the obligation to appoint a Grievance Officer applies ONLY to companies that?

A. Deal with sensitive personal data.

B. Conduct cross-border data transfers.

C. Are considered part of the public sector.

D. Lack alternate enforcement mechanisms.

Suggested Answer: *A*

Community vote distribution

A (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: A

Grievance Officers
Required by IT Act 43A and Rule 5(9)
Located at company dealing with SPI.
Handles any discrepancies and grievances of the provider of info with respect to processing of information in a time bound manner.
Must redress within one month.

upvoted 1 times

Bhimesh 5 months, 2 weeks ago

Selected Answer: A

Grievance Officers in companies (IT Act section 43A and rule 5(9))
Any company in India that deals with 'sensitive personal information' must 'address any discrepancies and grievances of their provider of the information with respect to processing of information in a time bound manner', and must appoint 'a Grievance Officer who shall redress the grievances… `within one month'.
A Grievance Officer is therefore the first tier of complaint handling in this system, one element of the role of a Data Protection Officer in proposals currently under consideration in the EU.
There are limitations on the scope of the obligation: it applies only to companies that deal with 'Sensitive Personal Data', not any personal information; data subjects can only use the provision where they have provided the information to the company; and Grievance Officers need not deal with them in relation to personal information obtained from other sources.

upvoted 1 times

Bhimesh 5 months, 2 weeks ago

Rule 5: Data Protection Principles
(9) Complaint handling
- No obligation to address and respond to complaints.
- Company must designate Grievance Officer (and publish name and contact details on website), who must redress within 1 month.

upvoted 1 times

Question #40 *Topic 1*

Section 43A of India's IT Rules 2011 requires which of the following for a privacy policy?

A. It should be available and produced on request.

B. It should be published on the website of the body corporate.

C. It should be emailed or faxed to data providers by the body corporate.

D. It should be shown to the data provider at the time of data collection.

Suggested Answer: *A*

Community vote distribution

B (100%)

Bhimesh 5 months, 3 weeks ago

Answer B - Rule 4 imposes a duty on Body Corporates seeking sensitive personal data to draft a privacy policy and make it easily accessible for people who are providing the information. The privacy policy should be clearly published on the website of the body corporate and should contain details on the type of information that is being collected, the purpose for which it has been collected and the reasonable security practices that have been undertaken to maintain the confidentiality of such information.

upvoted 1 times

rhyst1921 5 months, 4 weeks ago

Selected Answer: B

Rule 4 provides that the every body corporate that deals with sensitive personal data or information must have a privacy policy which shall be published on its website and provide for:

- clear and easily accessible statements of its practice and policies
- types of SPDI collected
- purpose
- disclosure
- RSPP

upvoted 1 times

TERENCELEE 1 year, 3 months ago

The privacy policy should be clearly published on the website of the body corporate and should contain details on the type of information that is being collected, the purpose for which it has been collected and the reasonable security practices that have been undertaken to maintain the confidentiality of such information.

upvoted 2 times

Question #41 *Topic 1*

All of the following are exempt from Section 43A of India's IT Rules 2011 EXCEPT?

A. Charitable groups.

B. Sole proprietorships.

C. Government agencies.

D. Religious organizations.

Suggested Answer: *C*

Community vote distribution

B (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: B

(i) Limitation to 'body corporate' and 'commercial or professional activities'.
Section 43A - only APPLIES to a 'body corporate', which 'means any company and includes a firm, SOLE PROPRIETORSHIP or other association of individuals engaged in commercial or professional activities'.

Religious and social organizations, including charities, whose activities are not classified as 'Commercial' will also be a substantial exclusion from the scope of the law.

Although there are some public sector bodies which come within this, such as state-owned corporations, there is very limited coverage of the public sector.

upvoted 1 times

Bhimesh 5 months, 2 weeks ago

All of India's right to information laws contained exemptions provisions. In the Central Act, section 8(1) lists all of the exemptions. Below is a general discussion of the exemption provisions:
• National Security or Sovereignty:
• National Economic Interests:
• Relations with Foreign States:
• Law Enforcement and the Judicial Process:
• Cabinet and Other Decision-Making Documents:
• Trade Secrets and Commercial Confidentiality:
• Personal Privacy:
• Individual Safety:
It is extremely positive that the Central Act makes all of the exemptions contained in section 8(1) subject to a "Public Interest Override" (see section 8(2) of the Central Act). What this means is that even where requested information is covered by an exemption, the information should still be disclosed to the applicant if the public interest in the specific case requires it.

upvoted 1 times

rhyst1921 5 months, 4 weeks ago

Selected Answer: B

Only religious, social and charitable organisations and non-commercial organisations (such as government agencies) that do not engage in activities classified as "commercial" (hence not within the scope of "body corporate" in section 43A) are exempted from section 43A of the IT Act.

upvoted 1 times

rhyst1921 5 months, 4 weeks ago

Selected Answer: B

Only activities that are not classified as "commercial" are not within the scope of "body corporate" in section 43A and hence exempt from section 43A.
Religious and social, charitable organisations and government agencies do not engage in commercial activities hence are exempt.

upvoted 1 times

Achatterjee 1 year ago

Selected Answer: B

It is B. Sole Proprietorship

upvoted 2 times

Question #42 *Topic 1*

SCENARIO – Please use the following to answer the next question:
Bharat Medicals is an established retail chain selling medical goods, with a presence in a number of cities throughout India. Their strategic partnership with major hospitals in these cities helped them capture an impressive market share over the years. However, with lifestyle and demographic shifts in India, the company saw a huge opportunity in door-to-door delivery of essential medical products. The need for such a service was confirmed by an independent consumer survey the firm conducted recently.
The company has launched their e-commerce platform in three metro cities, and plans to expand to the rest of the country in the future. Consumers need to register on the company website before they can make purchases. They are required to enter details such as name, age, address, telephone number, sex, date of birth and nationality – information that is stored on the company's servers. (Consumers also have the option of keeping their credit card number on file, so that it does not have to be entered every time they make payment.) If ordered items require a prescription, that authorization needs to be uploaded as well. The privacy notice explicitly requires that the consumer confirm that he or she is either the patient or has consent of the patient for uploading the health information. After creating a unique user ID and password, the consumer's registration will be confirmed through a text message sent to their listed mobile number.
To remain focused on their core business, Bharat outsourced the packaging, product dispatch and delivery activities to a third party firm, Maurya Logistics Ltd., with which it has a contractual agreement. It shares with Maurya Logistics the consumer name, address and other product-related details at the time of every purchase.
If consumers underwent medical treatment at one of the partner hospitals and consented to having their data transferred, their order requirement will be sent to their Bharat Medicals account directly, thereby doing away with the need to manually place an order for the medications.
Bharat Medicals takes regulatory compliance seriously; to ensure data privacy, it displays a privacy notice at the time of registration, and includes all the information that it collects. At this stage of their business, the company plans to store consumer information indefinitely, since the percentage of repeat customers and the frequency of orders per customer is still uncertain.
When collecting personal data, Bharat Medicals does NOT need to inform the consumer of what?

A. The recipients of the collected data.

B. The name of the body collecting the data.

C. The type of safeguards protecting the data.

D. The options the subject has to access his data.

Suggested Answer: *D*

Community vote distribution

D (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: D

5. Collection of information.
— (3) While collecting information directly from the person concerned, the body corporate or any person on its behalf snail take such steps as are, in the circumstances, reasonable to ensure that the person concerned is having the KNOWLEDGE of
— (a) the fact that the information is being collected;
(b) the purpose for which the information is being collected;
(c) the intended recipients of the information;
and (d) the name and address of — (i) the agency that is collecting the information; and (ii) the agency that will retain the information.
(8) Body corporate or any person on its behalf shall keep the information secure as provided in rule 8
upvoted 1 times

rhyst1921 5 months, 4 weeks ago

Selected Answer: D

A and B: Required under rule 5(3)
C: Required under rule 4 (Provide privacy policy that states, inter alia, the reasonable security practices and procedures)
upvoted 1 times

Question #43 *Topic 1*

SCENARIO – Please use the following to answer the next question:
Bharat Medicals is an established retail chain selling medical goods, with a presence in a number of cities throughout India. Their strategic partnership with major hospitals in these cities helped them capture an impressive market share over the years. However, with lifestyle and demographic shifts in India, the company saw a huge opportunity in door-to-door delivery of essential medical products. The need for such a service was confirmed by an independent consumer survey the firm conducted recently.
The company has launched their e-commerce platform in three metro cities, and plans to expand to the rest of the country in the future. Consumers need to register on the company website before they can make purchases. They are required to enter details such as name, age, address, telephone number, sex, date of birth and nationality – information that is stored on the company's servers. (Consumers also have the option of keeping their credit card number on file, so that it does not have to be entered every time they make payment.) If ordered items require a prescription, that authorization needs to be uploaded as well. The privacy notice explicitly requires that the consumer confirm that he or she is either the patient or has consent of the patient for uploading the health information. After creating a unique user ID and password, the consumer's registration will be confirmed through a text message sent to their listed mobile number.
To remain focused on their core business, Bharat outsourced the packaging, product dispatch and delivery activities to a third party firm, Maurya Logistics Ltd., with which it has a contractual agreement. It shares with Maurya Logistics the consumer name, address and other product-related details at the time of every purchase.
If consumers underwent medical treatment at one of the partner hospitals and consented to having their data transferred, their order requirement will be sent to their Bharat Medicals account directly, thereby doing away with the need to manually place an order for the medications.
Bharat Medicals takes regulatory compliance seriously; to ensure data privacy, it displays a privacy notice at the time of registration, and includes all the information that it collects. At this stage of their business, the company plans to store consumer information indefinitely, since the percentage of repeat customers and the frequency of orders per customer is still uncertain.
Which type of information collected by Bharat Medicals is considered sensitive personal information under the Information Technology Rules?

A. Prescription details.

B. Location data.

C. Nationality.

D. Religion.

Suggested Answer: *A*

Community vote distribution

A (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: A

A. Prescription details.

upvoted 1 times

Bhimesh 5 months, 3 weeks ago

Sensitive Personal Information (IN)

IN– Password; financial info; physical, physiological, or mental health; sexual orientation; medical records and history; biometrics; any detail of the above as provided to a corporate entity for providing services; any of the info receive above for storing or processing under lawful contracts.

upvoted 1 times

Question #44 *Topic 1*

SCENARIO – Please use the following to answer the next question:
Bharat Medicals is an established retail chain selling medical goods, with a presence in a number of cities throughout India. Their strategic partnership with major hospitals in these cities helped them capture an impressive market share over the years. However, with lifestyle and demographic shifts in India, the company saw a huge opportunity in door-to-door delivery of essential medical products. The need for such a service was confirmed by an independent consumer survey the firm conducted recently.
The company has launched their e-commerce platform in three metro cities, and plans to expand to the rest of the country in the future. Consumers need to register on the company website before they can make purchases. They are required to enter details such as name, age, address, telephone number, sex, date of birth and nationality – information that is stored on the company's servers. (Consumers also have the option of keeping their credit card number on file, so that it does not have to be entered every time they make payment.) If ordered items require a prescription, that authorization needs to be uploaded as well. The privacy notice explicitly requires that the consumer confirm that he or she is either the patient or has consent of the patient for uploading the health information. After creating a unique user ID and password, the consumer's registration will be confirmed through a text message sent to their listed mobile number.
To remain focused on their core business, Bharat outsourced the packaging, product dispatch and delivery activities to a third party firm, Maurya Logistics Ltd., with which it has a contractual agreement. It shares with Maurya Logistics the consumer name, address and other product-related details at the time of every purchase.
If consumers underwent medical treatment at one of the partner hospitals and consented to having their data transferred, their order requirement will be sent to their Bharat Medicals account directly, thereby doing away with the need to manually place an order for the medications.
Bharat Medicals takes regulatory compliance seriously; to ensure data privacy, it displays a privacy notice at the time of registration, and includes all the information that it collects. At this stage of their business, the company plans to store consumer information indefinitely, since the percentage of repeat customers and the frequency of orders per customer is still uncertain.
If a patient withdraws consent provided to one of the partner hospitals regarding the transfer of their data, which of the following would be true?

A. The patient cannot purchase medications from Bharat Medicals.

B. The hospital has the right to refuse withdrawal of consent since it has a partnership with Bharat Medicals.

C. The hospital will obtain the necessary medications from Bharat Medicals and provide them directly to patient.

D. The patient can buy medications from Bharat Medicals by uploading prescription to the Bharat Medicals website.

Suggested Answer: *D*

Community vote distribution

D (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: D

Patient may have withdrawn the consent provided to one of the partner hospitals regarding the transfer of their data - Bharat Medical's e-commerce platform with door-to-door delivery facility and tie- up with strategic partnership with major hospitals in India , patient can upload the prescription along with authorization, because the consent with Bharat medicals is still valid

upvoted 1 times

Question #45 *Topic 1*

SCENARIO – Please use the following to answer the next question:
Bharat Medicals is an established retail chain selling medical goods, with a presence in a number of cities throughout India. Their strategic partnership with major hospitals in these cities helped them capture an impressive market share over the years. However, with lifestyle and demographic shifts in India, the company saw a huge opportunity in door-to-door delivery of essential medical products. The need for such a service was confirmed by an independent consumer survey the firm conducted recently.
The company has launched their e-commerce platform in three metro cities, and plans to expand to the rest of the country in the future. Consumers need to register on the company website before they can make purchases. They are required to enter details such as name, age, address, telephone number, sex, date of birth and nationality – information that is stored on the company's servers. (Consumers also have the option of keeping their credit card number on file, so that it does not have to be entered every time they make payment.) If ordered items require a prescription, that authorization needs to be uploaded as well. The privacy notice explicitly requires that the consumer confirm that he or she is either the patient or has consent of the patient for uploading the health information. After creating a unique user ID and password, the consumer's registration will be confirmed through a text message sent to their listed mobile number.
To remain focused on their core business, Bharat outsourced the packaging, product dispatch and delivery activities to a third party firm, Maurya Logistics Ltd., with which it has a contractual agreement. It shares with Maurya Logistics the consumer name, address and other product-related details at the time of every purchase.
If consumers underwent medical treatment at one of the partner hospitals and consented to having their data transferred, their order requirement will be sent to their Bharat Medicals account directly, thereby doing away with the need to manually place an order for the medications.
Bharat Medicals takes regulatory compliance seriously; to ensure data privacy, it displays a privacy notice at the time of registration, and includes all the information that it collects. At this stage of their business, the company plans to store consumer information indefinitely, since the percentage of repeat customers and the frequency of orders per customer is still uncertain.
Which of the following is NOT true for Maurya Logistics?

A. It must have a privacy policy on its website describing its data processing practices.

B. It must obtain consent from Bharat Medicals consumers before processing their data.

C. It must process Bharat Medicals' consumer data only according to agreed contractual terms.

D. It must protect any unauthorized access any of Bharat Medicals consumer data that it obtained.

Suggested Answer: *B*

Community vote distribution

B (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: B

Data subject consent

Maurya Logistics is a processor and Bharat Medicals is a controller, the controller takes care of consent part.

Maurya Logistics will be looking after the following functions - packaging, product dispatch and delivery

Data Intermediary -

The Data Intermediary is referred to differently depending upon the country or jurisdiction. In Singapore, it is data intermediary.

In EU – the data processor,
And in the United States / India – a data processor is typically referred to as a vendor, service provider or a third-party service provider.
upvoted 1 times

Question #46 *Topic 1*

In India's IT Rules 2011, which is included in the definition of "sensitive personal data"?

A. Tax records.

B. IP addresses.

C. Next of kin.

D. Sexual Orientation.

Suggested Answer: *D*

Community vote distribution

D (100%)

Bhimesh 5 months, 2 weeks ago

Selected Answer: D

3. Sensitive personal data or information.— Sensitive personal data or information of a person means such personal information which consists of information relating to;—
(i) password;
(ii) financial information such as Bank account or credit card or debit card or other payment instrument details ;
(iii) physical, physiological and mental health condition;
(iv) sexual orientation;
(v) medical records and history;
(vi) Biometric information;
(vii) any detail relating to the above clauses as provided to body corporate for providing service; and
(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:
provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

upvoted 1 times

rhyst1921 5 months, 4 weeks ago

Selected Answer: D

Passwords, Financial information, physical or mental or physiological conditions,sexual orientation, medical records and history and biometric data provided that the information is not freely available/accessible in public domain or furnished under the Right to Information Act

upvoted 1 times