DUMPSARENA

Certified Information Privacy Manager

IAPP CIPM

Version Demo

Total Demo Questions: 10

Total Premium Questions: 166

Buy Premium PDF

https://dumpsarena.com

sales@dumpsarena.com

QUESTION NO: 1

If done correctly, how can a Data Protection Impact Assessment (DPIA) create a win/win scenario for organizations and individuals?

A. By quickly identifying potentially problematic data attributes and reducing the risk exposure.

B. By allowing Data Controllers to solicit feedback from individuals about how they feel about the potential data processing.

C. By enabling Data Controllers to be proactive in their analysis of processing activities and ensuring compliance with the law.

D. By better informing about the risks associated with the processing activity and improving the organization's transparency with individuals.

ANSWER: D

Explanation:

A Data Protection Impact Assessment (DPIA) is a process that organizations use to evaluate the potential risks associated with a specific data processing activity, and to identify and implement measures to mitigate those risks. By conducting a DPIA, organizations can proactively identify and address potential privacy concerns before they become a problem, and ensure compliance with data protection laws and regulations.

When organizations are transparent about their data processing activities and the risks associated with them, individuals are better informed about how their personal data is being used and can make more informed decisions about whether or not to provide their personal data. This creates a win/win scenario for organizations and individuals, as organizations are able to continue processing personal data in a compliant and transparent manner, while individuals are able to trust that their personal data is being used responsibly.

Additionally, by engaging with individuals in the DPIA process and soliciting their feedback, organizations can better understand the potential impact of their data processing activities on individuals and take steps to mitigate any negative impacts.

Reference: -https://iapp.org/news/a/privacy-pros-take-note-the-gdpr-is-coming-for-your-dpia/

-https://ec.europa.eu/info/publications/data-protection-impact-assessment-dpia-guidelines_en -https://gdpr-info.eu/art-35-gdpr/

QUESTION NO: 2

SCENARIO

Please use the following to answer the next QUESTION:

It's just what you were afraid of. Without consulting you, the information technology director at your organization launched a new initiative to encourage employees to use personal devices for conducting business. The initiative made purchasing a new, high-specification laptop computer an attractive option, with discounted laptops paid for as a payroll deduction spread over a year of paychecks. The organization is also paying the sales taxes. It's a great deal, and after a month, more than half the organization's employees have signed on and acquired new laptops. Walking through the facility, you see them happily customizing and comparing notes on their new computers, and at the end of the day, most take their laptops with them,

potentially carrying personal data to their homes or other unknown locations. It's enough to give you data- protection nightmares, and you've pointed out to the information technology Director and many others in the organization the potential hazards of this new practice, including the inevitability of eventual data loss or theft.

Today you have in your office a representative of the organization's marketing department who shares with you, reluctantly, a story with potentially serious consequences. The night before, straight from work, with laptop in hand, he went to the Bull and Horn Pub to play billiards with his friends. A fine night of sport and socializing began, with the laptop "safely" tucked on a bench, beneath his jacket. Later that night, when it was time to depart, he retrieved the jacket, but the laptop was gone. It was not beneath the bench or on another bench nearby. The waitstaff had not seen it. His friends were not playing a joke on him. After a sleepless night, he confirmed it this morning, stopping by the pub to talk to the cleanup crew. They had not found it. The laptop was missing. Stolen, it seems. He looks at you, embarrassed and upset.

You ask him if the laptop contains any personal data from clients, and, sadly, he nods his head, yes. He believes it contains files on about 100 clients, including names, addresses and governmental identification numbers. He sighs and places his head in his hands in despair.

From a business standpoint, what is the most productive way to view employee use of personal equipment for work-related tasks?

A. The use of personal equipment is a cost-effective measure that leads to no greater security risks than are always present in a modern organization.

B. Any computer or other equipment is company property whenever it is used for company business.

C. While the company may not own the equipment, it is required to protect the business-related data on any equipment used by its employees.

D. The use of personal equipment must be reduced as it leads to inevitable security risks.

ANSWER: C

QUESTION NO: 3

SCENARIO

Please use the following to answer the next QUESTION:

As they company’s new chief executive officer, Thomas Goddard wants to be known as a leader in data protection. Goddard recently served as the chief financial officer of Hoopy.com, a pioneer in online video viewing with millions of users around the world. Unfortunately, Hoopy is infamous within privacy protection circles for its ethically questionable practices, including unauthorized sales of personal data to marketers. Hoopy also was the target of credit card data theft that made headlines around the world, as at least two million credit card numbers were thought to have been pilfered despite the company’s claims that “appropriate” data protection safeguards were in place. The scandal affected the company’s business as competitors were quick to market an increased level of protection while offering similar entertainment and media content. Within three weeks after the scandal broke, Hoopy founder and CEO Maxwell Martin, Goddard’s mentor, was forced to step down.

Goddard, however, seems to have landed on his feet, securing the CEO position at your company, Medialite, which is just emerging from its start-up phase. He sold the company’s board and investors on his vision of Medialite building its brand partly on the basis of industry-leading data protection standards and procedures. He may have been a key part of a lapsed or even rogue organization in matters of privacy but now he claims to be reformed and a true believer in privacy protection. In his first week on the job, he calls you into his office and explains that your primary work responsibility is to bring his vision for privacy to life. But you also detect some reservations. “We want Medialite to have absolutely the highest standards,” he says. “In fact, I want us to be able to say that we are the clear industry leader in privacy and data protection. However, I also

need to be a responsible steward of the company's finances. So, while I want the best solutions across the board, they also need to be cost effective."

You are told to report back in a week's time with your recommendations. Charged with this ambiguous mission, you depart the executive suite, already considering your next steps.

You are charged with making sure that privacy safeguards are in place for new products and initiatives. What is the best way to do this?

A. Hold a meeting with stakeholders to create an interdepartmental protocol for new initiatives

B. Institute Privacy by Design principles and practices across the organization

C. Develop a plan for introducing privacy protections into the product development stage

D. Conduct a gap analysis after deployment of new products, then mend any gaps that are revealed

ANSWER: C

QUESTION NO: 4

An organization's privacy officer was just notified by the benefits manager that she accidentally sent out the retirement enrollment report of all employees to a wrong vendor.

Which of the following actions should the privacy officer take first?

A. Perform a risk of harm analysis.

B. Report the incident to law enforcement.

C. Contact the recipient to delete the email.

D. Send firm-wide email notification to employees.

ANSWER: A

QUESTION NO: 5

Data retention and destruction policies should meet all of the following requirements EXCEPT?

A. Data destruction triggers and methods should be documented.

B. Personal information should be retained only for as long as necessary to perform its stated purpose.

C. Documentation related to audit controls (third-party or internal) should be saved in a non-permanent format by default.

D. The organization should be documenting and reviewing policies of its other functions to ensure alignment (e.g. HR, business development, finance, etc.).

ANSWER: C

QUESTION NO: 6

SCENARIO

Please use the following to answer the next QUESTION:

Amira is thrilled about the sudden expansion of NatGen. As the joint Chief Executive Officer (CEO) with her long-time business partner Sadie, Amira has watched the company grow into a major competitor in the green energy market. The current line of products includes wind turbines, solar energy panels, and equipment for geothermal systems. A talented team of developers means that NatGen's line of products will only continue to grow.

With the expansion, Amira and Sadie have received advice from new senior staff members brought on to help manage the company's growth. One recent suggestion has been to combine the legal and security functions of the company to ensure observance of privacy laws and the company's own privacy policy. This sounds overly complicated to Amira, who wants departments to be able to use, collect, store, and dispose of customer data in ways that will best suit their needs. She does not want administrative oversight and complex structuring to get in the way of people doing innovative work.

Sadie has a similar outlook. The new Chief Information Officer (CIO) has proposed what Sadie believes is an unnecessarily long timetable for designing a new privacy program. She has assured him that NatGen will use the best possible equipment for electronic storage of customer and employee data. She simply needs a list of equipment and an estimate of its cost. But the CIO insists that many issues are necessary to consider before the company gets to that stage.

Regardless, Sadie and Amira insist on giving employees space to do their jobs. Both CEOs want to entrust the monitoring of employee policy compliance to low-level managers. Amira and Sadie believe these managers can adjust the company privacy policy according to what works best for their particular departments. NatGen's CEOs know that flexible interpretations of the privacy policy in the name of promoting green energy would be highly unlikely to raise any concerns with their customer base, as long as the data is always used in course of normal business activities.

Perhaps what has been most perplexing to Sadie and Amira has been the CIO's recommendation to institute a privacy compliance hotline. Sadie and Amira have relented on this point, but they hope to compromise by allowing employees to take turns handling reports of privacy policy violations. The implementation will be easy because the employees need no special preparation. They will simply have to document any concerns they hear.

Sadie and Amira are aware that it will be challenging to stay true to their principles and guard against corporate culture strangling creativity and employee morale. They hope that all senior staff will see the benefit of trying a unique approach.

What Data Lifecycle Management (DLM) principle should the company follow if they end up allowing departments to interpret the privacy policy differently?

A. Prove the authenticity of the company's records.

B. Arrange for official credentials for staff members.

C. Adequately document reasons for inconsistencies.

D. Create categories to reflect degrees of data importance.

ANSWER: C

QUESTION NO: 7

Which of the following is an example of Privacy by Design (PbD)?

A. A company hires a professional to structure a privacy program that anticipates the increasing demands of new laws.

B. The human resources group develops a training program for employees to become certified in privacy policy.

C. A labor union insists that the details of employers' data protection methods be documented in a new contract.

D. The information technology group uses privacy considerations to inform the development of new networking software.

ANSWER: C

QUESTION NO: 8

SCENARIO

Please use the following to answer the next QUESTION:

Perhaps Jack Kelly should have stayed in the U.S. He enjoys a formidable reputation inside the company, Special Handling Shipping, for his work in reforming certain "rogue" offices. Last year, news broke that a police sting operation had revealed a drug ring operating in the Providence, Rhode Island office in the United States. Video from the office's video surveillance cameras leaked to news operations showed a drug exchange between Special Handling staff and undercover officers.

In the wake of this incident, Kelly had been sent to Providence to change the "hands off" culture that upper management believed had let the criminal elements conduct their illicit transactions. After a few weeks under Kelly's direction, the office became a model of efficiency and customer service. Kelly monitored his workers' activities using the same cameras that had recorded the illegal conduct of their former co-workers.

Now Kelly has been charged with turning around the office in Cork, Ireland, another trouble spot. The company has received numerous reports of the staff leaving the office unattended. When Kelly arrived, he found that even when present, the staff often spent their days socializing or conducting personal business on their mobile phones. Again, he observed their behaviors using surveillance cameras. He issued written reprimands to six staff members based on the first day of video alone.

Much to Kelly's surprise and chagrin, he and the company are now under investigation by the Data Protection Commissioner of Ireland for allegedly violating the privacy rights of employees. Kelly was told that the

company's license for the cameras listed facility security as their main use, but he does not know why this matters. He has pointed out to his superiors that the company's training programs on privacy protection and data collection mention nothing about surveillance video.

You are a privacy protection consultant, hired by the company to assess this incident, report on the legal and compliance issues, and recommend next steps.

What should you advise this company regarding the status of security cameras at their offices in the United States?

A. Add security cameras at facilities that are now without them.

B. Set policies about the purpose and use of the security cameras.

C. Reduce the number of security cameras located inside the building.

D. Restrict access to surveillance video taken by the security cameras and destroy the recordings after a designated period of time.

ANSWER: B

QUESTION NO: 9

SCENARIO

Please use the following to answer the next QUESTION:

It's just what you were afraid of. Without consulting you, the information technology director at your organization launched a new initiative to encourage employees to use personal devices for conducting business. The initiative made purchasing a new, high-specification laptop computer an attractive option, with discounted laptops paid for as a payroll deduction spread over a year of paychecks. The organization is also paying the sales taxes. It's a great deal, and after a month, more than half the organization's employees have signed on and acquired new laptops. Walking through the facility, you see them happily customizing and comparing notes on their new computers, and at the end of the day, most take their laptops with them, potentially carrying personal data to their homes or other unknown locations. It's enough to give you data- protection nightmares, and you've pointed out to the information technology Director and many others in the organization the potential hazards of this new practice, including the inevitability of eventual data loss or theft.

Today you have in your office a representative of the organization's marketing department who shares with you, reluctantly, a story with potentially serious consequences. The night before, straight from work, with laptop in hand, he went to the Bull and Horn Pub to play billiards with his friends. A fine night of sport and socializing began, with the laptop "safely" tucked on a bench, beneath his jacket. Later that night, when it was time to depart, he retrieved the jacket, but the laptop was gone. It was not beneath the bench or on another bench nearby. The waitstaff had not seen it. His friends were not playing a joke on him. After a sleepless night, he confirmed it this morning, stopping by the pub to talk to the cleanup crew. They had not found it. The laptop was missing. Stolen, it seems. He looks at you, embarrassed and upset.

You ask him if the laptop contains any personal data from clients, and, sadly, he nods his head, yes. He believes it contains files on about 100 clients, including names, addresses and governmental identification numbers. He sighs and places his head in his hands in despair.

In order to determine the best course of action, how should this incident most productively be viewed?

A. As the accidental loss of personal property containing data that must be restored.

B. As a potential compromise of personal information through unauthorized access.

C. As an incident that requires the abrupt initiation of a notification campaign.

D. As the premeditated theft of company data, until shown otherwise.

ANSWER: B

QUESTION NO: 10

Which of the following best supports implementing controls to bring privacy policies into effect?

A. The internal audit department establishing the audit controls which test for policy effectiveness.

B. The legal department or outside counsel conducting a thorough review of the privacy program and policies.

C. The Chief Information Officer as part of the Senior Management Team creating enterprise privacy policies to ensure controls are available.

D. The information technology (IT) group supporting and enhancing the privacy program and privacy policy by developing processes and controls.

ANSWER: A