[UPDATED 2024 Getting CIPT Certification Made Easy! [Q58-Q80

[UPDATED 2024 Getting CIPT Certification Made Easy! CIPT Exam Crack Test Engine Dumps Training With 222 Questions NO.58 Which of these is considered an ethical dark pattern on privacy?
* Using attractive designs to influence an individual.
* Rewarding users for providing more personal information
* Giving users more privacy options in relation to their personal information
* Providing dear and simple privacy notices to users
rewarding users for providing more personal information is considered an unethical dark pattern on privacy. Dark patterns are user interface design choices that are intended to manipulate users into taking actions they might not otherwise take.

NO.59 SCENARIO

Please use the following to answer the next questions:

Your company is launching a new track and trace health app during the outbreak of a virus pandemic in the US. The developers claim the app is based on privacy by design because personal data collected was considered to ensure only necessary data is captured, users are presented with a privacy notice, and they are asked to give consent before data is shared. Users can update their consent after logging into an account, through a dedicated privacy and consent hub. This is accessible through the ‘Settings’ icon from any app page, then clicking ‘My Preferences’, and selecting ‘Information Sharing and Consent’ where the following choices are displayed:

* “I consent to receive notifications and infection alerts”;

* “I consent to receive information on additional features or services, and new products”;

* “I consent to sharing only my risk result and location information, for exposure and contact tracing purposes”;

* “I consent to share my data for medical research purposes”; and

* “I consent to share my data with healthcare providers affiliated to the company”.

For each choice, an ON* or OFF tab is available The default setting is ON for all Users purchase a virus screening service for USS29 99 for themselves or others using the app The virus screening service works as follows:

* Step 1 A photo of the user’s face is taken.

* Step 2 The user measures their temperature and adds the reading in the app

* Step 3 The user is asked to read sentences so that a voice analysis can detect symptoms

* Step 4 The user is asked to answer questions on known symptoms

* Step 5 The user can input information on family members (name date of birth, citizenship, home address, phone number, email and relationship).) The results are displayed as one of the following risk status “Low. “Medium” or “High” if the user is deemed at “Medium ” or “High” risk an alert may be sent to other users and the user is Invited to seek a medical consultation and diagnostic from a healthcare provider.

A user’s risk status also feeds a world map for contact tracing purposes, where users are able to check if they have been or are in dose proximity of an infected person If a user has come in contact with another individual classified as “medium’ or ‘high’ risk an instant notification also alerts the user of this. The app collects location trails of every user to monitor locations visited by an infected individual Location is collected using the phone’s GPS functionary, whether the app is in use or not however, the exact location of the user is “blurred’ for privacy reasons Users can only see on the map circles What is likely to be the biggest privacy concern with the current ‘Information Sharing and Consent’ page?
* The ON or OFF default setting for each item.
* The navigation needed in the app to get to the consent page.
* The option to consent to receive potential marketing information.
* The information sharing with healthcare providers affiliated with the company.
The biggest privacy concern with the current ‘Information Sharing and Consent’ page is that all consent options are set to ON by default. According to privacy by design principles and data protection regulations, such as the General Data Protection Regulation (GDPR), consent should be freely given, specific, informed, and unambiguous. Pre-ticked boxes do not constitute valid consent because they do not provide a clear affirmative action from the user. The default ON setting could lead to unintentional data sharing and potential privacy breaches, making this a significant concern. (Reference: IAPP CIPT Study Guide, Chapter on Privacy by Design and Default)

NO.60 What is the term for information provided to a social network by a member?
* Profile data.
* Declared data.
* Personal choice data.
* Identifier information.
The term for information provided to a social network by a member is as follows:

* Option A: Profile data.

* This is too broad and can include various types of information.

* Option B: Declared data.

* Declared data specifically refers to the information that a user explicitly provides to a social network, such as their name, age, location, and other personal details.

* Option C: Personal choice data.

* This is not a standard term in the context of social networks.

* Option D: Identifier information.

* This term is more general and can refer to any information that can identify an individual, not just the information provided by a user to a social network.

NO.61 SCENARIO

WebTracker Limited is a cloud-based online marketing service located in London. Last year, WebTracker migrated its IT infrastructure to the cloud provider AmaZure, which provides SQL Databases and Artificial Intelligence services to WebTracker. The roles and responsibilities between the two companies have been formalized in a standard contract, which includes allocating the role of data controller to WebTracker.

The CEO of WebTracker, Mr. Bond, would like to assess the effectiveness of AmaZure’s privacy controls, and he recently decided to hire you as an independent auditor. The scope of the engagement is limited only to the marketing services provided by WebTracker, you will not be evaluating any internal data processing activity, such as HR or Payroll.

This ad-hoc audit was triggered due to a future partnership between WebTracker and SmartHome – a partnership that will not require any data sharing. SmartHome is based in the USA, and most recently has dedicated substantial resources to developing smart refrigerators that can suggest the recommended daily calorie intake based on DNA information. This and other personal data is collected by WebTracker.

To get an idea of the scope of work involved, you have decided to start reviewing the company’s documentation and interviewing key staff to understand potential privacy risks.

The results of this initial work include the following notes:

* There are several typos in the current privacy notice of WebTracker, and you were not able to find the privacy notice for SmartHome.

* You were unable to identify all the sub-processors working for SmartHome. No subcontractor is indicated in the cloud agreement with AmaZure, which is responsible for the support and maintenance of the cloud infrastructure.

* There are data flows representing personal data being collected from the internal employees of WebTracker, including an interface from the HR system.

* Part of the DNA data collected by WebTracker was from employees, as this was a prototype approved by the CEO of WebTracker.

* All the WebTracker and SmartHome customers are based in USA and Canada.

Which of the following issues is most likely to require an investigation by the Chief Privacy Officer (CPO) of WebTracker?
* Data flows use encryption for data at rest, as defined by the IT manager.
* AmaZure sends newsletter to WebTracker customers, as approved by the Marketing Manager.
* Employees’ personal data are being stored in a cloud HR system, as approved by the HR Manager.
* File Integrity Monitoring is being deployed in SQL servers, as indicated by the IT Architect Manager.
Explanation/Reference:

NO.62 An EU marketing company is planning to make use of personal data captured to make automated decisions based on profiling. In some cases, processing and automated decisions may have a legal effect on individuals, such as credit worthiness.

When evaluating the implementation of systems making automated decisions, in which situation would the company have to accommodate an individual’s right NOT to be subject to such processing to ensure compliance under the General Data Protection Regulation (GDPR)?
* When an individual’s legal status or rights are not affected by the decision.
* When there is no human intervention or influence in the decision-making process.
* When the individual has given explicit consent to such processing and suitable safeguards exist.
* When the decision is necessary for entering into a contract and the individual can contest the decision.
Under the GDPR, individuals have the right not to be subject to a decision based solely on automated processing, including profiling, if it produces legal effects concerning them or significantly affects them. This right applies particularly when there is no human intervention in the decision-making process. The GDPR Article 22 specifies that individuals can object to automated decisions that have significant consequences unless the decision is necessary for entering into a contract, authorized by law, or based on explicit consent with appropriate safeguards. Therefore, the company’s systems making automated decisions without human involvement must accommodate individuals’ rights to opt out to ensure compliance. This interpretation is aligned with GDPR regulations as explained in IAPP’s Information Privacy Technologist materials.

NO.63 SCENARIO

Clean-Q is a company that offers house-hold and office cleaning services. The company receives requests from consumers via their website and telephone, to book cleaning services. Based on the type and size of service, Clean-Q then contracts individuals that are registered on its resource database – currently managed in- house by Clean-Q IT Support. Because of Clean-Q’s business model, resources are contracted as needed instead of permanently employed.

The table below indicates some of the personal information Clean-Q requires as part of its business operations:

Category	Types of Personal Information
Customers	Name, address (location), contact information, billing information
Resources (contracted)	Name, contact information, banking details, address

premium.validexam.com

Clean-Q has an internal employee base of about 30 people. A recent privacy compliance exercise has been conducted to align employee data management and human resource functions with applicable data protection regulation. Therefore, the Clean-Q permanent employee base is not included as part of this scenario.

With an increase in construction work and housing developments, Clean-Q has had an influx of requests for cleaning services. The demand has overwhelmed Clean-Q’s traditional supply and demand system that has caused some overlapping bookings.

Ina business strategy session held by senior management recently, Clear-Q invited vendors to present potential solutions to their current operational issues. These vendors included Application developers and Cloud-Q’s solution providers, presenting their proposed solutions and platforms.

The Managing Director opted to initiate the process to integrate Clean-Q’s operations with a cloud solution (LeadOps) that will provide the following solution one single online platform: A web interface that Clean-Q accesses for the purposes of resource and customer management. This would entail uploading resource and customer information.

* A customer facing web interface that enables customers to register, manage and submit cleaning service requests online.

* A resource facing web interface that enables resources to apply and manage their assigned jobs.

* An online payment facility for customers to pay for services.

If Clean-Q were to utilize LeadOps’ services, what is a contract clause that may be included in the agreement entered into with LeadOps?
* A provision that holds LeadOps liable for a data breach involving Clean-Q’s information.
* A provision prescribing technical and organizational controls that LeadOps must implement.
* A provision that requires LeadOps to notify Clean-Q of any suspected breaches of information that involves customer or resource information managed on behalf of Clean-Q.
* A provision that allows Clean-Q to conduct audits of LeadOps’ information processing and information security environment, at LeadOps’ cost and at any time that Clean-Q requires.

NO.64 SCENARIO

Please use the following to answer the next question:

Chuck, a compliance auditor for a consulting firm focusing on healthcare clients, was required to travel to the client’s office to perform an onsite review of the client’s operations. He rented a car from Finley Motors upon arrival at the airport as so he could commute to and from the client’s office. The car rental agreement was electronically signed by Chuck and included his name, address, driver’s license, make/model of the car, billing rate, and additional details describing the rental transaction. On the second night, Chuck was caught by a red light camera not stopping at an intersection on his way to dinner. Chuck returned the car back to the car rental agency at the end week without mentioning the infraction and Finley Motors emailed a copy of the final receipt to the address on file.

Local law enforcement later reviewed the red light camera footage. As Finley Motors is the registered owner of the car, a notice was sent to them indicating the infraction and fine incurred. This notice included the license plate number, occurrence date and time, a photograph of the driver, and a web portal link to a video clip of the violation for further review. Finley Motors, however, was not responsible for the violation as they were not driving the car at the time and transferred the incident to AMP Payment Resources for further review. AMP Payment Resources identified Chuck as the driver based on the rental agreement he signed when picking up the car and then contacted Chuck directly through a written letter regarding the infraction to collect the fine.

After reviewing the incident through the AMP Payment Resources’ web portal, Chuck paid the fine using his personal credit card. Two weeks later, Finley Motors sent Chuck an email promotion offering 10% off a future rental.

What is the strongest method for authenticating Chuck’s identity prior to allowing access to his violation information through the AMP Payment Resources web portal?
* By requiring Chuck use the last 4 digits of his driver’s license number in combination with a unique PIN provided within the violation notice.
* By requiring Chuck use his credit card number in combination with the last 4 digits of his driver’s license.

* By requiring Chuck use the rental agreement number in combination with his email address.
* By requiring Chuck to call AMP Payment Resources directly and provide his date of birth and home address.

NO.65 Which activity would best support the principle of data quality?
* Providing notice to the data subject regarding any change in the purpose for collecting such data.
* Ensuring that the number of teams processing personal information is limited.
* Delivering information in a format that the data subject understands.
* Ensuring that information remains accurate.
Explanation

Explanation/Reference: https://iapp.org/resources/article/fair-information-practices/

NO.66 Users of a web-based email service have their accounts breached through compromised login credentials. Which possible consequences of the breach illustrate the two categories of Calo’s Harm Dimensions?
* Financial loss and blackmail.
* Financial loss and solicitation.
* Identity theft and embarrassment.
* Identity theft and the leaking of information.

NO.67 Which of the following is the best method to minimize tracking through the use of cookies?
* Use ‘private browsing’ mode and delete checked files, clear cookies and cache once a day.
* Install a commercially available third-party application on top of the browser that is already installed.
* Install and use a web browser that is advertised as ‘built specifically to safeguard user privacy’.
* Manage settings in the browser to limit the use of cookies and remove them once the session completes.

NO.68 A user who owns a resource wants to give other individuals access to the resource. What control would apply?
* Mandatory access control.
* Role-based access controls.
* Discretionary access control.
* Context of authority controls.
Explanation/Reference: https://docs.microsoft.com/bs-latn-ba/azure/role-based-access-control/overview

NO.69 What is the main benefit of using dummy data during software testing?
* The data comes in a format convenient for testing.
* Statistical disclosure controls are applied to the data.
* The data enables the suppression of particular values in a set.
* Developers do not need special privacy training to test the software.

NO.70 Which of the following is a privacy consideration for NOT sending large-scale SPAM type emails to a database of email addresses?
* Poor user experience.
* Emails are unsolicited.
* Data breach notification.
* Reduction in email deliverability score.
a privacy consideration for NOT sending large-scale SPAM type emails to a database of email addresses is that the emails are unsolicited. Sending unsolicited emails can violate individuals’ privacy rights and may also be illegal under certain anti-spam laws.

NO.71 What risk is mitigated when routing video traffic through a company’s application servers, rather than sending the video traffic directly from one user to another?

* The user is protected against phishing attacks.
* The user’s identity is protected from the other user.
* The user’s approximate physical location is hidden from the other user.
* The user is assured that stronger authentication methods have been used.
* Option A: Phishing attacks are typically related to email or messaging security rather than direct video traffic.

* Option B: While identity protection can be a factor, routing through company servers primarily obfuscates the user’s IP address and other metadata, which reveals physical location rather than identity specifics.

* Option C: Routing video traffic through a company’s servers hides the users’ IP addresses from each other, which prevents them from determining each other’s physical location.

* Option D: Stronger authentication methods are related to access control but not necessarily to the routing of video traffic.

References:

* IAPP CIPT Study Guide

* Network security principles related to traffic routing

NO.72 Which of the following became a foundation for privacy principles and practices of countries and organizations across the globe?
* The Personal Data Ordinance.
* The EU Data Protection Directive.
* The Code of Fair Information Practices.
* The Organization for Economic Co-operation and Development (OECD) Privacy Principles.

Reference:

The Organization for Economic Co-operation and Development (OECD) Privacy Principles became a foundation for privacy principles and practices of countries and organizations across the globe4. The OECD Privacy Principles were adopted by OECD member countries in 1980 as a set of eight basic principles for ensuring adequate protection of personal data across national borders4. The OECD Privacy Principles have been widely recognized as an international standard for data protection and have influenced many regional and national laws and frameworks4.

NO.73 Which is the most accurate type of biometrics?
* DNA.
* Voiceprint.
* Fingerprint.
* Facial recognition.

NO.74 Which of the following is NOT relevant to a user exercising their data portability rights?
* Notice and consent for the downloading of data.
* Detection of phishing attacks against the portability interface.
* Re-authentication of an account, including two-factor authentication as appropriate.
* Validation of users with unauthenticated identifiers (e.g. IP address, physical address).

NO.75 Which of the following is considered a records management best practice?
* Archiving expired data records and files.
* Storing decryption keys with their associated backup systems.
* Implementing consistent handling practices across all record types.

* Using classification to determine access rules and retention policy.
Records management best practices include classifying data to determine appropriate access controls and retention policies. Classification allows organizations to systematically identify and manage records according to their level of sensitivity and importance, ensuring that data is accessible only to authorized personnel and retained for the required duration. This practice helps in maintaining data security and compliance with legal and regulatory requirements. The IAPP documentation emphasizes the importance of data classification in establishing robust data governance frameworks (IAPP, “Records Management and Data Classification”).

NO.76 To meet data protection and privacy legal requirements that may require personal data to be disposed of or deleted when no longer necessary for the use it was collected, what is the best privacy-enhancing solution a privacy technologist should recommend be implemented in application design to meet this requirement?
* Implement a process to delete personal data on demand and maintain records on deletion requests.
* Implement automated deletion of off-site backup of personal data based on annual risk assessments.
* Develop application logic to validate and purge personal data according to legal hold status or retention schedule.
* Securely archive personal data not accessed or used in the last 6 months. Automate a quarterly review to delete data from archive once no longer needed.
To meet data protection and privacy legal requirements regarding the disposal or deletion of personal data when it is no longer necessary, the best privacy-enhancing solution involves integrating robust application logic. Option C suggests developing application logic that validates and purges personal data according to its legal hold status or retention schedule. This approach ensures compliance with legal mandates for data retention and deletion, minimizing the risk of retaining unnecessary personal data. References to this can be found in IAPP’s CIPT materials, specifically in the sections discussing data lifecycle management and legal compliance requirements.

NO.77 SCENARIO

You have just been hired by Ancillary.com, a seller of accessories for everything under the sun, including waterproof stickers for pool floats and decorative bands and cases for sunglasses. The company sells cell phone cases, e-cigarette cases, wine spouts, hanging air fresheners for homes and automobiles, book ends, kitchen implements, visors and shields for computer screens, passport holders, gardening tools and lawn ornaments, and catalogs full of health and beauty products. The list seems endless. As the CEO likes to say, Ancillary offers, without doubt, the widest assortment of low-price consumer products from a single company anywhere.

Ancillary’s operations are similarly diverse. The company originated with a team of sales consultants selling home and beauty products at small parties in the homes of customers, and this base business is still thriving.

However, the company now sells online through retail sites designated for industries and demographics, sites such as “My Cool Ride” for automobile-related products or “Zoomer” for gear aimed toward young adults.

The company organization includes a plethora of divisions, units and outrigger operations, as Ancillary has been built along a decentered model rewarding individual initiative and flexibility, while also acquiring key assets. The retail sites seem to all function differently, and you wonder about their compliance with regulations and industry standards. Providing tech support to these sites is also a challenge, partly due to a variety of logins and authentication protocols.

You have been asked to lead three important new projects at Ancillary:

The first is the personal data management and security component of a multi-faceted initiative to unify the company’s culture. For this project, you are considering using a series of third- party servers to provide company data and approved applications to employees.

The second project involves providing point of sales technology for the home sales force, allowing them to move beyond paper checks and manual credit card imprinting.

Finally, you are charged with developing privacy protections for a single web store housing all the company’s product lines as well as products from affiliates. This new omnibus site will be known, aptly, as “Under the Sun.” The Director of Marketing wants the site not only to sell Ancillary’s products, but to link to additional products from other retailers through paid advertisements. You need to brief the executive team of security concerns posed by this approach.

What technology is under consideration in the first project in this scenario?
* Server driven controls.
* Cloud computing
* Data on demand
* MAC filtering
The technology under consideration in the first project is cloud computing.

* Explanation:

* Cloud Computing: This involves using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer. This technology

* provides flexibility, scalability, and cost-effectiveness.

* Data Management and Security: Cloud services can unify data management across the company by providing a centralized platform where all employees can access approved applications and data securely.

* Third-Party Servers: Using third-party servers, a characteristic feature of cloud computing, aligns with the project’s goal to provide company data and approved applications to employees.

* Security Considerations: While cloud computing offers many advantages, it also requires careful attention to data security, including encryption, access controls, and regular security audits to protect sensitive information.

References:

* IAPP Privacy Management, Information Privacy Technologist Certification Textbooks

* NIST SP 800-145: The NIST Definition of Cloud Computing

NO.78 Which Organization for Economic Co-operation and Development (OECD) privacy protection principle encourages an organization to obtain an individual s consent before transferring personal information?
* Individual participation.
* Purpose specification.
* Collection limitation.
* Accountability.
The OECD privacy protection principle that encourages an organization to obtain an individual’s consent before transferring personal information is individual participation. This principle asserts that individuals should have the right to know about the collection and use of their personal data, and to consent to its transfer.

It emphasizes transparency and individual control over personal information (IAPP, Certified Information Privacy Technologist (CIPT) materials).

NO.79 What is an example of a just-in-time notice?

* A warning that a website may be unsafe.
* A full organizational privacy notice publicly available on a website
* A credit card company calling a user to verify a purchase before itis authorized
* Privacy information given to a user when he attempts to comment on an online article.

Explanation/Reference: https://www.clarip.com/data-privacy/just-time-notices/

NO.80 What is a main benefit of data aggregation?

* It is a good way to perform analysis without needing a statistician.
* It applies two or more layers of protection to a single data record.
* It allows one to draw valid conclusions from small data samples.
* It is a good way to achieve de-identification and unlinkabilty.

Explanation/Reference:

CIPT Exam Dumps Contains FREE Real Quesions from the Actual Exam:
https://www.validexam.com/CIPT-latest-dumps.html]