IAPP.CIPP-E.v2022-03-07.q101

Exam Code:	CIPP-E
Exam Name:	Certified Information Privacy Professional/Europe (CIPP/E)
Certification Provider:	IAPP
Free Question Number:	101
Version:	v2022-03-07
# of views:	2025
# of Questions views:	990
https://www.freepdfdumps.com/IAPP.CIPP-E.v2022-03-07.q101.html	

NEW QUESTION: 1
What is true of both the General Data Protection Regulation (GDPR) and the Council of Europe Convention 108?
A. Both govern the manual processing of personal data
B. Both only apply to European Union countries
C. Both govern international transfers of personal data
D. Both require notification of processing activities to a supervisory authority
Answer: (SHOW ANSWER)

NEW QUESTION: 2
According to the GDPR, what is the main task of a Data Protection Officer (DPO)?
A. To monitor compliance with other local or European data protection provisions.
B. To create and maintain records of processing activities.
C. To create procedures for notification of personal data breaches to competent supervisory authorities.
D. To conduct Privacy Impact Assessments on behalf of the controller or processor.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 3
SCENARIO
Please use the following to answer the next question:
Due to rapidly expanding workforce, Company A has decided to outsource its payroll function to Company B. Company B is an established payroll service provider with a sizable client base and a solid reputation in the industry.
Company B's payroll solution for Company A relies on the collection of time and attendance data obtained via a biometric entry system installed in each of Company A's factories. Company B won't hold any biometric data itself, but the related data will be uploaded to Company B's UK servers and used to provide the payroll service. Company B's live systems will contain the following information for each of Company A's employees:

Name
Address
Date of Birth
Payroll number
National Insurance number
Sick pay entitlement
Maternity/paternity pay entitlement
Holiday entitlement
Pension and benefits contributions
Trade union contributions
Jenny is the compliance officer at Company A.
She first considers whether Company A needs to carry out a data protection impact assessment in relation to the new time and attendance system, but isn't sure whether or not this is required.
Jenny does know, however, that under the GDPR there must be a formal written agreement requiring Company B to use the time and attendance data only for the purpose of providing the payroll service, and to apply appropriate technical and organizational security measures for safeguarding the data. Jenny suggests that Company B obtain advice from its data protection officer. The company doesn't have a DPO but agrees, in the interest of finalizing the contract, to sign up for the provisions in full. Company A enters into the contract.
Weeks later, while still under contract with Company A, Company B embarks upon a separate project meant to enhance the functionality of its payroll service, and engages Company C to help. Company C agrees to extract all personal data from Company B's live systems in order to create a new database for Company B. This database will be stored in a test environment hosted on Company C's U.S. server. The two companies agree not to include any data processing provisions in their services agreement, as data is only being used for IT testing purposes.
Unfortunately, Company C's U.S. server is only protected by an outdated IT security system, and suffers a cyber security incident soon after Company C begins work on the project. As a result, data relating to Company A's employees is visible to anyone visiting Company C's website. Company A is unaware of this until Jenny receives a letter from the supervisory authority in connection with the investigation that ensues. As soon as Jenny is made aware of the breach, she notifies all affected employees.
Under the GDPR, which of Company B's actions would NOT be likely to trigger a potential enforcement action?
A. Their engagement of Company C to improve their payroll service.
B. Their omission of data protection provisions in their contract with Company C.
C. Their failure to provide sufficient security safeguards to Company A's data.
D. Their decision to operate without a data protection officer.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 4
Data retention in the EU was underpinned by a legal framework established by the Data Retention Directive (2006/24/EC). Why is the Directive no longer part of EU law?

A. The Directive was annulled by the European Court of Human Rights.
B. The Directive was superseded by the EU Directive on Privacy and Electronic Communications.
C. The Directive was annulled by the Court of Justice of the European Union.
D. The Directive was superseded by the General Data Protection Regulation.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 5
In 2016's Guidance, the United Kingdom's Information Commissioner's Office (ICO) reaffirmed the importance of using a "layered notice" to provide data subjects with what?
A. An efficient means of providing written consent in member states where they are required to do so.
B. A privacy notice explaining the consequences for opting out of the use of cookies on a website.
C. An explanation of the security measures used when personal data is transferred to a third party.
D. A privacy notice containing brief information whilst offering access to further detail.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 6
SCENARIO
Please use the following to answer the next question:
Liem, an online retailer known for its environmentally friendly shoes, has recently expanded its presence in Europe. Anxious to achieve market dominance, Liem teamed up with another eco friendly company, EcoMick, which sells accessories like belts and bags. Together the companies drew up a series of marketing campaigns designed to highlight the environmental and economic benefits of their products. After months of planning, Liem and EcoMick entered into a data sharing agreement to use the same marketing database, MarketIQ, to send the campaigns to their respective contacts.
Liem and EcoMick also entered into a data processing agreement with MarketIQ, the terms of which included processing personal data only upon Liem and EcoMick's instructions, and making available to them all information necessary to demonstrate compliance with GDPR obligations.
Liem and EcoMick then procured the services of a company called JaphSoft, a marketing optimization firm that uses machine learning to help companies run successful campaigns. Clients provide JaphSoft with the personal data of individuals they would like to be targeted in each campaign. To ensure protection of its clients' data, JaphSoft implements the technical and organizational measures it deems appropriate. JaphSoft works to continually improve its machine learning models by analyzing the data it receives from its clients to determine the most successful components of a successful campaign. JaphSoft then uses such models in providing services to its client-base. Since the models improve only over a period of time as more information is collected, JaphSoft does not have a deletion process for the data it receives from clients. However, to ensure compliance with data privacy rules, JaphSoft pseudonymizes the personal data by removing identifying information from the contact information. JaphSoft's engineers, however, maintain all contact information in the same database as the identifying information.
Under its agreement with Liem and EcoMick, JaphSoft received access to MarketIQ, which included contact information as well as prior purchase history for such contacts, to create campaigns that would result in the most views of the two companies' websites. A prior Liem customer, Ms. Iman, received a marketing

campaign from JaphSoft regarding Liem's as well as EcoMick's latest products. While Ms. Iman recalls checking a box to receive information in the future regarding Liem's products, she has never shopped EcoMick, nor provided her personal data to that company.
JaphSoft's use of pseudonymization is NOT in compliance with the CDPR because?
A. JaphSoft failed to first anonymize the personal data.
B. JaphSoft pseudonymized all the data instead of deleting what it no longer needed.
C. JaphSoft failed to keep personally identifiable information in a separate database.
D. JaphSoft was in possession of information that could be used to identify data subjects.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 7
Based on GDPR Article 35, which of the following situations would trigger the need to complete a DPIA?
A. A company wants to combine location data with other data in order to offer more personalized service for the customer.
B. A company wants to use location data to infer information on a person's clothes purchasing habits.
C. A company wants to build a dating app that creates candidate profiles based on location data and data from third-party sources.
D. A company wants to use location data to track delivery trucks in order to make the routes more efficient.
Answer: (SHOW ANSWER)
Explanation/Reference: http://webcache.googleusercontent.com/search?q=cache:aQkU17eX9sQJ:https://www.shlegal.com/insights/article-29-data-protection-working-party-gdpr-guidelines-on-data-protection-impact- assessments&client=firefox-b-e&hl=en&gl=pk&strip=1&vwsrc=0

NEW QUESTION: 8
SCENARIO
Please use the following to answer the next question:
Joe started the Gummy Bear Company in 2000 from his home in Vermont, USA.
Today, it is a multi-billion-dollar candy company operating in every continent. All of the company's IT servers are located in Vermont. This year Joe hires his son Ben to join the company and head up Project Big, which is a major marketing strategy to triple gross revenue in just 5 years. Ben graduated with a PhD in computer software from a top university. Ben decided to join his father's company, but is also secretly working on launching a new global online dating website company called Ben Knows Best.
Ben is aware that the Gummy Bear Company has millions of customers and believes that many of them might also be interested in finding their perfect match. For Project Big, Ben redesigns the company's online web portal and requires customers in the European Union and elsewhere to provide additional personal information in order to remain a customer. Project Ben begins collecting data about customers' philosophical beliefs, political opinions and marital status.
If a customer identifies as single, Ben then copies all of that customer's personal data onto a separate database for Ben Knows Best. Ben believes that he is not doing anything wrong, because he explicitly asks each customer to give their consent by requiring them to check a box before accepting their information. As

Project Big is an important project, the company also hires a first year college student named Sam, who is studying computer science to help Ben out.
Ben calls out and Sam comes across the Ben Knows Best database. Sam is planning on going to Ireland over Spring Beak with 10 of his friends, so he copies all of the customer information of people that reside in Ireland so that he and his friends can contact people when they are in Ireland.
Joe also hires his best friend's daughter, Alice, who just graduated from law school in the U.S., to be the company's new General Counsel. Alice has heard about the GDPR, so she does some research on it. Alice approaches Joe and informs him that she has drafted up Binding Corporate Rules for everyone in the company to follow, as it is important for the company to have in place a legal mechanism to transfer data internally from the company's operations in the European Union to the U.S.
Joe believes that Alice is doing a great job, and informs her that she will also be in-charge of handling a major lawsuit that has been brought against the company in federal court in the U.S. To prepare for the lawsuit, Alice instructs the company's IT department to make copies of the computer hard drives from the entire global sales team, including the European Union, and send everything to her so that she can review everyone's information. Alice believes that Joe will be happy that she did the first level review, as it will save the company a lot of money that would otherwise be paid to its outside law firm.
In preparing the company for its impending lawsuit, Alice's instruction to the company's IT Department violated Article 5 of the GDPR because the company failed to first do what?
A. Encrypt the data from all of its employees.
B. Inform all of its employees about the lawsuit.
C. Minimize the amount of data collected for the lawsuit.
D. Send out consent forms to all of its employees.
Answer: (SHOW ANSWER)

NEW QUESTION: 9
SCENARIO
Please use the following to answer the next question:
Javier is a member of the fitness club EVERFIT. This company has branches in many EU member states, but for the purposes of the GDPR maintains its primary establishment in France. Javier lives in Newry, Northern Ireland (part of the U.K.), and commutes across the border to work in Dundalk, Ireland. Two years ago while on a business trip, Javier was photographed while working out at a branch of EVERFIT in Frankfurt, Germany. At the time, Javier gave his consent to being included in the photograph, since he was told that it would be used for promotional purposes only. Since then, the photograph has been used in the club's U.K. brochures, and it features in the landing page of its U.K. website. However, the fitness club has recently fallen into disrepute due to widespread mistreatment of members at various branches of the club in several EU member states. As a result, Javier no longer feels comfortable with his photograph being publicly associated with the fitness club.
After numerous failed attempts to book an appointment with the manager of the local branch to discuss this matter, Javier sends a letter to EVETFIT requesting that his image be removed from the website and all promotional materials. Months pass and Javier, having received no acknowledgment of his request,

becomes very anxious about this matter. After repeatedly failing to contact EVETFIT through alternate channels, he decides to take action against the company.
Javier contacts the U.K. Information Commissioner's Office ('ICO' - the U.K.'s supervisory authority) to lodge a complaint about this matter. The ICO, pursuant to Article 56 (3) of the GDPR, informs the CNIL (i.e. the supervisory authority of EVERFIT's main establishment) about this matter. Despite the fact that EVERFIT has an establishment in the U.K., the CNIL decides to handle the case in accordance with Article 60 of the GDPR. The CNIL liaises with the ICO, as relevant under the cooperation procedure. In light of issues amongst the supervisory authorities to reach a decision, the European Data Protection Board becomes involved and, pursuant to the consistency mechanism, issues a binding decision.
Additionally, Javier sues EVERFIT for the damages caused as a result of its failure to honor his request to have his photograph removed from the brochure and website.
Under the cooperation mechanism, what should the lead authority (the CNIL) do after it has formed its view on the matter?
A. Submit a draft decision directly to the Commission to ensure the effectiveness of the consistency mechanism.
B. Submit a draft decision to other supervisory authorities for their opinion.
C. Request that the other supervisory authorities provide the lead authority with a draft decision for its consideration.
D. Request that members of the seconding supervisory authority and the host supervisory authority co-draft a decision.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 10
What must be included in a written agreement between the controller and processor in relation to processing conducted on the controller's behalf?
A. An obligation on both parties to report any serious personal data breach to the supervisory authority.
B. An obligation on both parties to agree to a termination of the agreement if the other party is responsible for a personal data breach.
C. An obligation on the processor to report any personal data breach to the controller within 72 hours.
D. An obligation on the processor to assist the controller in complying with the controller's obligations to notify the supervisory authority about personal data breaches.
Answer: (SHOW ANSWER)

NEW QUESTION: 11
SCENARIO
Please use the following to answer the next question:
You have just been hired by a toy manufacturer based in Hong Kong. The company sells a broad range of dolls, action figures and plush toys that can be found internationally in a wide variety of retail stores. Although the manufacturer has no offices outside Hong Kong and in fact does not employ any staff outside Hong Kong, it has entered into a number of local distribution contracts. The toys produced by the company can be

found in all popular toy stores throughout Europe, the United States and Asia. A large portion of the company's revenue is due to international sales.
The company now wishes to launch a new range of connected toys, ones that can talk and interact with children. The CEO of the company is touting these toys as the next big thing, due to the increased possibilities offered: The figures can answer children's questions on various subjects, such as mathematical calculations or the weather. Each figure is equipped with a microphone and speaker and can connect to any smartphone or tablet via Bluetooth. Any mobile device within a 10-meter radius can connect to the toys via Bluetooth as well.
The figures can also be associated with other figures (from the same manufacturer) and interact with each other for an enhanced play experience.
When a child asks the toy a question, the request is sent to the cloud for analysis, and the answer is generated on cloud servers and sent back to the figure. The answer is given through the figure's integrated speakers, making it appear as though that the toy is actually responding to the child's question. The packaging of the toy does not provide technical details on how this works, nor does it mention that this feature requires an internet connection. The necessary data processing for this has been outsourced to a data center located in South Africa. However, your company has not yet revised its consumer-facing privacy policy to indicate this.
In parallel, the company is planning to introduce a new range of game systems through which consumers can play the characters they acquire in the course of playing the game. The system will come bundled with a portal that includes a Near-Field Communications (NFC) reader. This device will read an RFID tag in the action figure, making the figure come to life onscreen. Each character has its own stock features and abilities, but it is also possible to earn additional ones by accomplishing game goals. The only information stored in the tag relates to the figures' abilities. It is easy to switch characters during the game, and it is possible to bring the figure to locations outside of the home and have the character's abilities remain intact.
In light of the requirements of Article 32 of the GDPR (related to the Security of Processing), which practice should the company institute?
A. Encrypt the data in transit over the wireless Bluetooth connection.
B. Include dual-factor authentication before each use by a child in order to ensure a minimum amount of security.
C. Include three-factor authentication before each use by a child in order to ensure the best level of security possible.
D. Insert contractual clauses into the contract between the toy manufacturer and the cloud service provider, since South Africa is outside the European Union.
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 12
Which of the following describes a mandatory requirement for a group of undertakings that wants to appoint a single data protection officer?
A. The group of undertakings must be comprised of organizations of similar sizes and functions.
B. The group of undertakings must obtain approval from a supervisory authority.

C. The data protection officer must be easily accessible from each establishment where the undertakings are located.
D. The data protection officer must be located in the country where the data controller has its main establishment.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 13
What term BEST describes the European model for data protection?
A. Sectoral
B. Self-regulatory
C. Market-based
D. Comprehensive
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

NEW QUESTION: 14
SCENARIO
Please use the following to answer the next question:
Building Block Inc. is a multinational company, headquartered in Chicago with offices throughout the United States, Asia, and Europe (including Germany, Italy, France and Portugal). Last year the company was the victim of a phishing attack that resulted in a significant data breach. The executive board, in coordination with the general manager, their Privacy Office and the Information Security team, resolved to adopt additional security measures. These included training awareness programs, a cybersecurity audit, and use of a new software tool called SecurityScan, which scans employees' computers to see if they have software that is no longer being supported by a vendor and therefore not getting security updates. However, this software also provides other features, including the monitoring of employees' computers.
Since these measures would potentially impact employees, Building Block's Privacy Office decided to issue a general notice to all employees indicating that the company will implement a series of initiatives to enhance information security and prevent future data breaches.
After the implementation of these measures, server performance decreased. The general manager instructed the Security team on how to use SecurityScan to monitor employees' computers activity and their location. During these activities, the Information Security team discovered that one employee from Italy was daily connecting to a video library of movies, and another one from Germany worked remotely without authorization. The Security team reported these incidents to the Privacy Office and the general manager. In their report, the team concluded that the employee from Italy was the reason why the server performance decreased.
Due to the seriousness of these infringements, the company decided to apply disciplinary measures to both employees, since the security and privacy policy of the company prohibited employees from installing software on the company's computers, and from working remotely without authorization.

What would be the MOST APPROPRIATE way for Building Block to handle the situation with the employee from Italy?

A. Since the employee was not informed that the security measures would be used for other purposes such as monitoring, the company could face difficulties in applying any disciplinary measures to this employee.

B. Since this was a serious infringement, but the employee was not appropriately informed about the consequences the new security measures, the company would be entitled to apply some disciplinary measures, but not dismissal.

C. Since the GDPR does not apply to this situation, the company would be entitled to apply any disciplinary measure authorized under Italian labor law.

D. Since the employee was the cause of a serious risk for the server performance and their data, the company would be entitled to apply disciplinary measures to this employee, including fair dismissal.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 15

SCENARIO

Please use the following to answer the next Question: 01

Louis, a long-time customer of Bedrock Insurance, was involved in a minor car accident a few months ago. Although no one was hurt, Louis has been plagued by texts and calls from a company called Accidentable offering to help him recover compensation for personal injury. Louis has heard about insurance companies selling customers' data to third parties, and he's convinced that Accidentable must have gotten his information from Bedrock Insurance.

Louis has also been receiving an increased amount of marketing information from Bedrock, trying to sell him their full range of their insurance policies.

Perturbed by this, Louis has started looking at price comparison sites on the internet and has been shocked to find that other insurers offer much cheaper rates than Bedrock, even though he has been a loyal customer for many years. When his Bedrock policy comes up for renewal, he decides to switch to Zantrum Insurance.

In order to activate his new insurance policy, Louis needs to supply Zantrum with information about his No Claims bonus, his vehicle and his driving history. After researching his rights under the GDPR, he writes to ask Bedrock to transfer his information directly to Zantrum. He also takes this opportunity to ask Bedrock to stop using his personal data for marketing purposes.

Bedrock supplies Louis with a PDF and XML (Extensible Markup Language) versions of his No Claims Certificate, but tells Louis it cannot transfer his data directly to Zantrum as this is not technically feasible. Bedrock also explains that Louis's contract included a provision whereby Louis agreed that his data could be used for marketing purposes; according to Bedrock, it is too late for Louis to change his mind about this. It angers Louis when he recalls the wording of the contract, which was filled with legal jargon and very confusing.

In the meantime, Louis is still receiving unwanted calls from Accidentable Insurance. He writes to Accidentable to ask for the name of the organization that supplied his details to them. He warns Accidentable that he plans to complain to the data protection authority, because he thinks their company has been using his data unlawfully. His letter states that he does not want his data being used by them in any way.

Accidentable's response letter confirms Louis's suspicions. Accidentable is Bedrock Insurance's wholly owned subsidiary, and they received information about Louis's accident from Bedrock shortly after Louis submitted his accident claim. Accidentable assures Louis that there has been no breach of the GDPR, as Louis's contract included, a provision in which he agreed to share his information with Bedrock's affiliates for business purposes.
Louis is disgusted by the way in which he has been treated by Bedrock, and writes to them insisting that all his information be erased from their computer system.
Based on the GDPR's position on the use of personal data for direct marketing purposes, which of the following is true about Louis's rights as a data subject?
A. Louis has the right to object to the use of his data, unless his data is required by Bedrock for the purpose of exercising a legal claim.
B. Louis has the right to object at any time to the use of his data and Bedrock must honor his request to cease use.
C. Louis does not have the right to object to the use of his data if Bedrock can demonstrate compelling legitimate grounds for the processing.
D. Louis does not have the right to object to the use of his data because he previously consented to it.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 16
An online company's privacy practices vary due to the fact that it offers a wide variety of services. How could it best address the concern that explaining them all would make the policies incomprehensible?
A. Identify uses of data in a privacy notice mailed to the data subject.
B. Use a layered privacy notice on its website and in its email communications.
C. Provide only general information about its processing activities and offer a toll-free number for more information.
D. Place a banner on its website stipulating that visitors agree to its privacy policy and terms of use by visiting the site.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 17
SCENARIO
Please use the following to answer the next question:

Outliers Inc. is a travel service company which has lost substantial revenue over the last few years. Their new manager, Jonathan, suspects that this is partly due to the company's outdated website. After doing some research, he meets with a sales representative from the up-and-coming IT company ZenFiTech, hoping that they can design a new, cutting-edge website for Outliers Inc.'s foundering business.
During negotiations, a ZenFiTech representative describes a plan for gathering more customer information through detailed questionnaires, which could be used to tailor their preferences to specific travel destinations. Outliers Inc. can choose any number of data categories - age, income, ethnicity - that would help them best accomplish their goals. Jonathan loves this idea, but would also like to have some way of gauging how successful this approach is, especially since the questionnaires will require customers to provide explicit consent to having their data collected. The ZenFiTech representative suggests that they also run a program to analyze the new website's traffic, in order to get a better understanding of how customers are using it. He explains his plan to place a number of cookies on customer devices. The cookies will allow the company to collect IP addresses and other information, such as the sites from which the customers came, how much time they spend on the Outliers Inc. website, and which pages on the site they visit. All of this information will be compiled in log files, which ZenFiTech will analyze by means of a special program. Outliers Inc. would receive aggregate statistics to help them evaluate the website's effectiveness. Jonathan enthusiastically engages ZenFiTech for these services.
With regard to Outliers Inc.'s use of website cookies, which of the following statements is correct?
A. Because the use of cookies involves the potential for location tracking, explicit consent must be obtained from customers.
B. Because not all of the cookies are strictly necessary to enable the use of a service requested from Outliers Inc., consent requirements apply to their use of cookies.
C. Because of the categories of data involved, explicit consent for the use of cookies must be obtained separately from customers.
D. Because ZenFiTech will receive only aggregate statistics of data collected from the cookies, no additional consent is necessary.
Answer: (SHOW ANSWER)

NEW QUESTION: 18
SCENARIO
Please use the following to answer the next question:
WonderkKids provides an online booking service for childcare. Wonderkids is based in France, but hosts its website through a company in Switzerland. As part of their service, WonderKids will pass all personal data provided to them to the childcare provider booked through their system. The type of personal data collected on the website includes the name of the person booking the childcare, address and contact details, as well as information about the children to be cared for including name, age, gender and health information. The privacy statement on Wonderkids' website states the following:
"WonderkKids provides the information you disclose to us through this website to your childcare provider for scheduling and health and safety reasons. We may also use your and your child's personal information for our own legitimate business purposes and we employ a third-party website hosting company located in Switzerland to store the dat a. Any data stored on equipment located in Switzerland meets the European

Commission provisions for guaranteeing adequate safeguards for you and your child's personal information. We will only share you and your child's personal information with businesses that we see as adding real value to you. By providing us with any personal data, you consent to its transfer to affiliated businesses and to send you promotional offers."
"We may retain you and your child's personal information for no more than 28 days, at which point the data will be depersonalized, unless your personal information is being used for a legitimate business purpose beyond 28 days where it may be retained for up to 2 years."
"We are processing you and your child's personal information with your consent. If you choose not to provide certain information to us, you may not be able to use our services. You have the right to: request access to you and your child's personal information; rectify or erase you or your child's personal information; the right to correction or erasure of you and/or your child's personal information; object to any processing of you and your child's personal information. You also have the right to complain to the supervisory authority about our data processing activities." What must the contract between WonderKids and the hosting service provider contain?
A. Controller-to-controller model contract clauses.
B. A non-disclosure agreement.
C. Audit rights for the data subjects.
D. The requirement to implement technical and organizational measures to protect the data.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 19
What must a data controller do in order to make personal data pseudonymous?
A. Use the data only in aggregated form for research purposes.
B. Encrypt the data in order to prevent any unauthorized access or modification.
C. Separately hold any information that would allow linking the data to the data subject.
D. Remove all indirect data identifiers and dispose of them securely.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 20
Which of the following would NOT be relevant when determining if a processing activity would be considered profiling?
A. If the processing is used to predict the behavior of data subjects
B. If the processing is to be performed by a third-party vendor
C. If the processing involves data that is considered personal data
D. If the processing of the data is done through automated means
Answer: (SHOW ANSWER)

NEW QUESTION: 21
SCENARIO
Please use the following to answer the next question:

Joe is the new privacy manager for Who-R-U, a Canadian business that provides DNA analysis. The company is headquartered in Montreal, and all of its employees are located there. The company offers its services to Canadians only: Its website is in English and French, it accepts only Canadian currency, and it blocks internet traffic from outside of Canada (although this solution doesn't prevent all non-Canadian traffic). It also declines to process orders that request the DNA report to be sent outside of Canada, and returns orders that show a non-Canadian return address.
Bob, the President of Who-R-U, thinks there is a lot of interest for the product in the EU, and the company is exploring a number of plans to expand its customer base.
The first plan, collegially called We-Track-U, will use an app to collect information about its current Canadian customer base. The expansion will allow its Canadian customers to use the app while traveling abroad. He suggests that the company use this app to gather location information. If the plan shows promise, Bob proposes to use push notifications and text messages to encourage existing customers to pre-register for an EU version of the service. Bob calls this work plan, We-Text-U. Once the company has gathered enough pre-registrations, it will develop EU-specific content and services.
Another plan is called Customer for Life. The idea is to offer additional services through the company's app, like storage and sharing of DNA information with other applications and medical providers. The company's contract says that it can keep customer DNA indefinitely, and use it to offer new services and market them to customers. It also says that customers agree not to withdraw direct marketing consent. Paul, the marketing director, suggests that the company should fully exploit these provisions, and that it can work around customers' attempts to withdraw consent because the contract invalidates them.
The final plan is to develop a brand presence in the EU. The company has already begun this process. It is in the process of purchasing the naming rights for a building in Germany, which would come with a few offices that Who-R-U executives can use while traveling internationally. The office doesn't include any technology or infrastructure; rather, it's simply a room with a desk and some chairs.
On a recent trip concerning the naming-rights deal, Bob's laptop is stolen. The laptop held unencrypted DNA reports on 5,000 Who-R-U customers, all of whom are residents of Canad a. The reports include customer name, birthdate, ethnicity, racial background, names of relatives, gender, and occasionally health information.
If Who-R-U decides to track locations using its app, what must it do to comply with the GDPR?
A. Get consent from the app users.
B. Anonymize the data and add latency so it avoids disclosing real time locations.
C. Provide a transparent notice to users.
D. Obtain a court order because location data is a special category of personal data.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 22
Which aspect of the GDPR will likely have the most impact on the consistent implementation of data protection laws throughout the European Union?
A. That it makes appointment of a data protection officer mandatory
B. That it takes the form of a Regulation as opposed to a Directive
C. That it makes notification of large-scale data breaches mandatory

D. That it essentially functions as a one-stop shop mechanism
Answer: A (LEAVE A REPLY)

NEW QUESTION: 23
Which judicial body makes decisions on actions taken by individuals wishing to enforce their rights under EU law?
A. Court of Auditors
B. European Court of Human Rights
C. Court of Justice of European Union
D. European Data Protection Board
Answer: (SHOW ANSWER)

NEW QUESTION: 24
SCENARIO
Please use the following to answer the next question:
TripBliss Inc. is a travel service company which has lost substantial revenue over the last few years. Their new manager, Oliver, suspects that this is partly due to the company's outdated website. After doing some research, he meets with a sales representative from the up-and-coming IT company Techiva, hoping that they can design a new, cutting-edge website for TripBliss Inc.'s foundering business.
During negotiations, a Techiva representative describes a plan for gathering more customer information through detailed questionnaires, which could be used to tailor their preferences to specific travel destinations. TripBliss Inc. can choose any number of data categories - age, income, ethnicity - that would help them best accomplish their goals. Oliver loves this idea, but would also like to have some way of gauging how successful this approach is, especially since the questionnaires will require customers to provide explicit consent to having their data collected. The Techiva representative suggests that they also run a program to analyze the new website's traffic, in order to get a better understanding of how customers are using it. He explains his plan to place a number of cookies on customer devices. The cookies will allow the company to collect IP addresses and other information, such as the sites from which the customers came, how much time they spend on the TripBliss Inc. website, and which pages on the site they visit. All of this information will be compiled in log files, which Techiva will analyze by means of a special program. TripBliss Inc. would receive aggregate statistics to help them evaluate the website's effectiveness. Oliver enthusiastically engages Techiva for these services.
Techiva assigns the analytics portion of the project to longtime account manager Leon Santos. As is standard practice, Leon is given administrator rights to TripBliss Inc.'s website, and can authorize access to the log files gathered from it. Unfortunately for TripBliss Inc., however, Leon is taking on this new project at a time when his dissatisfaction with Techiva is at a high point. In order to take revenge for what he feels has been unfair treatment at the hands of the company, Leon asks his friend Fred, a hobby hacker, for help. Together they come up with the following plan: Fred will hack into Techiva's system and copy their log files onto a USB stick.
Despite his initial intention to send the USB to the press and to the data protection authority in order to denounce Techiva, Leon experiences a crisis of conscience and ends up reconsidering his plan. He decides

instead to securely wipe all the data from the USB stick and inform his manager that the company's system of access control must be reconsidered.
If TripBliss Inc. decides not to report the incident to the supervisory authority, what would be their BEST defense?
A. The incident resulted from the actions of a third-party that were beyond their control.
B. The sensitivity of the categories of data involved in the incident was not substantial enough.
C. The destruction of the stolen data makes any risk to the affected data subjects unlikely.
D. The resulting obligation to notify data subjects would involve disproportionate effort.
Answer: (SHOW ANSWER)

NEW QUESTION: 25
Which of the following countries will continue to enjoy adequacy status under the GDPR, pending any future European Commission decision to the contrary?
A. Greece
B. Switzerland
C. Norway
D. Australia
Answer: B (LEAVE A REPLY)

NEW QUESTION: 26
Tanya is the Data Protection Officer for Curtains Inc., a GDPR data controller. She has recommended that the company encrypt all personal data at rest. Which GDPR principle is she following?
A. Accuracy
B. Storage Limitation
C. Integrity and confidentiality
D. Lawfulness, fairness and transparency
Answer: (SHOW ANSWER)
Explanation/Reference: https://www.icaew.com/technical/technology/data/data-protection/data-protection-articles/do-i-have- to-encrypt-personal-data-to-comply-with-dpa-2018

NEW QUESTION: 27
SCENARIO
Please use the following to answer the next question:
Louis, a long-time customer of Bedrock Insurance, was involved in a minor car accident a few months ago. Although no one was hurt, Louis has been plagued by texts and calls from a company called Accidentable offering to help him recover compensation for personal injury. Louis has heard about insurance companies selling customers' data to third parties, and he's convinced that Accidentable must have gotten his information from Bedrock Insurance.
Louis has also been receiving an increased amount of marketing information from Bedrock, trying to sell him their full range of their insurance policies.

Perturbed by this, Louis has started looking at price comparison sites on the internet and has been shocked to find that other insurers offer much cheaper rates than Bedrock, even though he has been a loyal customer for many years. When his Bedrock policy comes up for renewal, he decides to switch to Zantrum Insurance. In order to activate his new insurance policy, Louis needs to supply Zantrum with information about his No Claims bonus, his vehicle and his driving history. After researching his rights under the GDPR, he writes to ask Bedrock to transfer his information directly to Zantrum. He also takes this opportunity to ask Bedrock to stop using his personal data for marketing purposes.

Bedrock supplies Louis with a PDF and XML (Extensible Markup Language) versions of his No Claims Certificate, but tells Louis it cannot transfer his data directly to Zantrum as this is not technically feasible. Bedrock also explains that Louis's contract included a provision whereby Louis agreed that his data could be used for marketing purposes; according to Bedrock, it is too late for Louis to change his mind about this. It angers Louis when he recalls the wording of the contract, which was filled with legal jargon and very confusing.

In the meantime, Louis is still receiving unwanted calls from Accidentable Insurance. He writes to Accidentable to ask for the name of the organization that supplied his details to them. He warns Accidentable that he plans to complain to the data protection authority, because he thinks their company has been using his data unlawfully. His letter states that he does not want his data being used by them in any way.

Accidentable's response letter confirms Louis's suspicions. Accidentable is Bedrock Insurance's wholly owned subsidiary, and they received information about Louis's accident from Bedrock shortly after Louis submitted his accident claim. Accidentable assures Louis that there has been no breach of the GDPR, as Louis's contract included, a provision in which he agreed to share his information with Bedrock's affiliates for business purposes.

Louis is disgusted by the way in which he has been treated by Bedrock, and writes to them insisting that all his information be erased from their computer system.

After Louis has exercised his right to restrict the use of his data, under what conditions would Accidentable have grounds for refusing to comply?

A. If Accidentable also uses the data to conduct public health research.

B. If the accuracy of the data is not an aspect that Louis is disputing.

C. If Accidentable is entitled to use of the data as an affiliate of Bedrock.

D. If the data becomes necessary to defend Accidentable's legal rights.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 28

SCENARIO

Please use the following to answer the next question:

Due to rapidly expanding workforce, Company A has decided to outsource its payroll function to Company B. Company B is an established payroll service provider with a sizable client base and a solid reputation in the industry.

Company B's payroll solution for Company A relies on the collection of time and attendance data obtained via a biometric entry system installed in each of Company A's factories. Company B won't hold any biometric

data itself, but the related data will be uploaded to Company B's UK servers and used to provide the payroll service. Company B's live systems will contain the following information for each of Company A's employees:
Name
Address
Date of Birth
Payroll number
National Insurance number
Sick pay entitlement
Maternity/paternity pay entitlement
Holiday entitlement
Pension and benefits contributions
Trade union contributions
Jenny is the compliance officer at Company A.
She first considers whether Company A needs to carry out a data protection impact assessment in relation to the new time and attendance system, but isn't sure whether or not this is required.
Jenny does know, however, that under the GDPR there must be a formal written agreement requiring Company B to use the time and attendance data only for the purpose of providing the payroll service, and to apply appropriate technical and organizational security measures for safeguarding the data. Jenny suggests that Company B obtain advice from its data protection officer. The company doesn't have a DPO but agrees, in the interest of finalizing the contract, to sign up for the provisions in full. Company A enters into the contract.
Weeks later, while still under contract with Company A, Company B embarks upon a separate project meant to enhance the functionality of its payroll service, and engages Company C to help. Company C agrees to extract all personal data from Company B's live systems in order to create a new database for Company B. This database will be stored in a test environment hosted on Company C's U.S. server. The two companies agree not to include any data processing provisions in their services agreement, as data is only being used for IT testing purposes.
Unfortunately, Company C's U.S. server is only protected by an outdated IT security system, and suffers a cyber security incident soon after Company C begins work on the project. As a result, data relating to Company A's employees is visible to anyone visiting Company C's website. Company A is unaware of this until Jenny receives a letter from the supervisory authority in connection with the investigation that ensues. As soon as Jenny is made aware of the breach, she notifies all affected employees.
The GDPR requires sufficient guarantees of a company's ability to implement adequate technical and organizational measures. What would be the most realistic way that Company B could have fulfilled this requirement?
A. Hiring companies whose measures are consistent with recommendations of accrediting bodies.
B. Avoiding the use of another company's data to improve their own services.
C. Requesting advice and technical support from Company A's IT team.
D. Vetting companies' measures with the appropriate supervisory authority.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 29

SCENARIO

Please use the following to answer the next question:

The fitness company Vigotron has recently developed a new app called M-Health, which it wants to market on its website as a free download. Vigotron's marketing manager asks his assistant Emily to create a webpage that describes the app and specifies the terms of use. Emily, who is new at Vigotron, is excited about this task. At her previous job she took a data protection class, and though the details are a little hazy, she recognizes that Vigotron is going to need to obtain user consent for use of the app in some cases. Emily sketches out the following draft, trying to cover as much as possible before sending it to Vigotron's legal department.

Registration Form

Vigotron's new M-Health app makes it easy for you to monitor a variety of health-related activities, including diet, exercise, and sleep patterns. M-Health relies on your smartphone settings (along with other third-party apps you may already have) to collect data about all of these important lifestyle elements, and provide the information necessary for you to enrich your quality of life. (Please click here to read a full description of the services that M-Health provides.) Vigotron values your privacy. The M-Heaith app allows you to decide which information is stored in it, and which apps can access your dat a. When your device is locked with a passcode, all of your health and fitness data is encrypted with your passcode. You can back up data stored in the Health app to Vigotron's cloud provider, Stratculous. (Read more about Stratculous here.) Vigotron will never trade, rent or sell personal information gathered from the M-Health app. Furthermore, we will not provide a customer's name, email address or any other information gathered from the app to any third- party without a customer's consent, unless ordered by a court, directed by a subpoena, or to enforce the manufacturer's legal rights or protect its business or property.

We are happy to offer the M-Health app free of charge. If you want to download and use it, we ask that you first complete this registration form. (Please note that use of the M-Health app is restricted to adults aged 16 or older, unless parental consent has been given to minors intending to use it.) First name:

Surname:

Year of birth:

Email:

Physical Address (optional*):

Health status:

*If you are interested in receiving newsletters about our products and services that we think may be of interest to you, please include your physical address. If you decide later that you do not wish to receive these newsletters, you can unsubscribe by sending an email to unsubscribe@vigotron.com or send a letter with your request to the address listed at the bottom of this page.

Terms and Conditions

1. Jurisdiction. [...]
2. Applicable law. [...]
3. Limitation of liability. [...]

Consent

By completing this registration form, you attest that you are at least 16 years of age, and that you consent to the processing of your personal data by Vigotron for the purpose of using the M-Health app. Although you are entitled to opt out of any advertising or marketing, you agree that Vigotron may contact you or provide you with any required notices, agreements, or other information concerning the services by email or other electronic means. You also agree that the Company may send automated emails with alerts regarding any problems with the M-Health app that may affect your well being.
If a user of the M-Health app were to decide to withdraw his consent, Vigotron would first be required to do what?
A. Inform any third parties of the user's withdrawal of consent.
B. Cease processing any data collected through use of the app.
C. Erase any data collected from the time the app was first used.
D. Provide the user with logs of data collected through use of the app.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 30
What permissions are required for a marketer to send an email marketing message to a consumer in the EU?
A. A prior opt-in consent for consumers unless they are already customers.
B. A pre-checked box stating that the consumer agrees to receive email marketing.
C. A notice that the consumer's email address will be used for marketing purposes.
D. No prior permission required, but an opt-out requirement on all emails sent to consumers.
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://www.forbes.com/sites/forbescommunicationscouncil/2018/06/27/what-gdpr-means-for- email-marketing-to-eu-customers/#64020aa8374a

NEW QUESTION: 31
SCENARIO
Please use the following to answer the next question:
Ben is a member of the fitness club STAYFIT. This company has branches in many EU member states, but for the purposes of the GDPR maintains its primary establishment in France. Ben lives in Newry, Northern Ireland (part of the U.K.), and commutes across the border to work in Dundalk, Ireland. Two years ago while on a business trip, Ben was photographed while working out at a branch of STAYFIT in Frankfurt, Germany. At the time, Ben gave his consent to being included in the photograph, since he was told that it would be used for promotional purposes only. Since then, the photograph has been used in the club's U.K. brochures, and it features in the landing page of its U.K. website. However, the fitness club has recently fallen into disrepute due to widespread mistreatment of members at various branches of the club in several EU member states. As a result, Ben no longer feels comfortable with his photograph being publicly associated with the fitness club.
After numerous failed attempts to book an appointment with the manager of the local branch to discuss this matter, Ben sends a letter to STAYFIT requesting that his image be removed from the website and all promotional materials. Months pass and Ben, having received no acknowledgment of his request, becomes

very anxious about this matter. After repeatedly failing to contact STAYFIT through alternate channels, he decides to take action against the company.
Ben contacts the U.K. Information Commissioner's Office ('ICO' - the U.K.'s supervisory authority) to lodge a complaint about this matter.
Under the cooperation mechanism, what should the lead authority (the CNIL) do after it has formed its view on the matter?
A. Request that members of the seconding supervisory authority and the host supervisory authority co-draft a decision.
B. Request that the other supervisory authorities provide the lead authority with a draft decision for its consideration.
C. Submit a draft decision directly to the Commission to ensure the effectiveness of the consistency mechanism.
D. Submit a draft decision to other supervisory authorities for their opinion.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 32
According to the GDPR, how is pseudonymous personal data defined?
A. Data that can no longer be attributed to a specific data subject without the use of additional information kept separately.
B. Data that can no longer be attributed to a specific data subject, with no possibility of re-identifying the data.
C. Data that has been rendered anonymous in such a manner that the data subject is no longer identifiable.
D. Data that has been encrypted or is subject to other technical safeguards.
Answer: (SHOW ANSWER)
Explanation/Reference: https://www.chino.io/blog/what-is-pseudonymous-data-according-to-the-gdpr/

NEW QUESTION: 33
SCENARIO
Please use the following to answer the next question:
Ben is a member of the fitness club STAYFIT. This company has branches in many EU member states, but for the purposes of the GDPR maintains its primary establishment in France. Ben lives in Newry, Northern Ireland (part of the U.K.), and commutes across the border to work in Dundalk, Ireland. Two years ago while on a business trip, Ben was photographed while working out at a branch of STAYFIT in Frankfurt, Germany.

At the time, Ben gave his consent to being included in the photograph, since he was told that it would be used for promotional purposes only. Since then, the photograph has been used in the club's U.K. brochures, and it features in the landing page of its U.K. website. However, the fitness club has recently fallen into disrepute due to widespread mistreatment of members at various branches of the club in several EU member states. As a result, Ben no longer feels comfortable with his photograph being publicly associated with the fitness club.

After numerous failed attempts to book an appointment with the manager of the local branch to discuss this matter, Ben sends a letter to STAYFIT requesting that his image be removed from the website and all promotional materials. Months pass and Ben, having received no acknowledgment of his request, becomes very anxious about this matter. After repeatedly failing to contact STAYFIT through alternate channels, he decides to take action against the company.

Ben contacts the U.K. Information Commissioner's Office ('ICO' - the U.K.'s supervisory authority) to lodge a complaint about this matter.

Assuming that multiple STAYFIT branches across several EU countries are acting as separate data controllers, and that each of those branches were responsible for mishandling Ben's request, how may Ben proceed in order to seek compensation?

A. He will have to sue the STAYFIT's head office in France, where STAYFIT has its main establishment.

B. He will be able to sue any one of the relevant STAYFIT branches, as each one may be held liable for the entire damage.

C. He will have to sue each STAYFIT branch so that each branch provides proportionate compensation commensurate with its contribution to the damage or distress suffered by Ben.

D. He will be able to apply to the European Data Protection Board in order to determine which particular STAYFIT branch is liable for damages, based on the decision that was made by the board.

Answer: A (LEAVE A REPLY)

Explanation/Reference:

NEW QUESTION: 34

SCENARIO

Please use the following to answer the next question:

Building Block Inc. is a multinational company, headquartered in Chicago with offices throughout the United States, Asia, and Europe (including Germany, Italy, France and Portugal). Last year the company was the victim of a phishing attack that resulted in a significant data breach. The executive board, in coordination with the general manager, their Privacy Office and the Information Security team, resolved to adopt additional security measures. These included training awareness programs, a cybersecurity audit, and use of a new software tool called SecurityScan, which scans employees' computers to see if they have software that is no longer being supported by a vendor and therefore not getting security updates. However, this software also provides other features, including the monitoring of employees' computers.

Since these measures would potentially impact employees, Building Block's Privacy Office decided to issue a general notice to all employees indicating that the company will implement a series of initiatives to enhance information security and prevent future data breaches.

After the implementation of these measures, server performance decreased. The general manager instructed the Security team on how to use SecurityScan to monitor employees' computers activity and their location. During these activities, the Information Security team discovered that one employee from Italy was daily connecting to a video library of movies, and another one from Germany worked remotely without authorization.
The Security team reported these incidents to the Privacy Office and the general manager. In their report, the team concluded that the employee from Italy was the reason why the server performance decreased.
Due to the seriousness of these infringements, the company decided to apply disciplinary measures to both employees, since the security and privacy policy of the company prohibited employees from installing software on the company's computers, and from working remotely without authorization.
What would be the MOST APPROPRIATE way for Building Block to handle the situation with the employee from Italy?
A. Since the employee was the cause of a serious risk for the server performance and their data, the company would be entitled to apply disciplinary measures to this employee, including fair dismissal.
B. Since the employee was not informed that the security measures would be used for other purposes such as monitoring, the company could face difficulties in applying any disciplinary measures to this employee.
C. Since the GDPR does not apply to this situation, the company would be entitled to apply any disciplinary measure authorized under Italian labor law.
D. Since this was a serious infringement, but the employee was not appropriately informed about the consequences the new security measures, the company would be entitled to apply some disciplinary measures, but not dismissal.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 35
In addition to the European Commission, who can adopt standard contractual clauses, assuming that all required conditions are met?
A. Approved data controllers.
B. The Council of the European Union.
C. National data protection authorities.
D. The European Data Protection Supervisor.
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/ standard-contractual-clauses-scc_en

NEW QUESTION: 36
Which mechanism, new to the GDPR, now allows for the possibility of personal data transfers to third countries under Article 42?
A. Standard contractual clauses.
B. Approved certifications.
C. Law enforcement requests.
D. Binding corporate rules.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 37
Under Article 80(1) of the GDPR, individuals can elect to be represented by not-for-profit organizations in a privacy group litigation or class action. These organizations are commonly known as?
A. Law firm organizations.
B. Human rights organizations.
C. Civil society organizations.
D. Constitutional rights organizations.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 38
SCENARIO
Please use the following to answer the next question:
T-Craze, a German-headquartered specialty t-shirt company, was successfully selling to large German metropolitan cities. However, after a recent merger with another German-based company that was selling to a broader European market, T-Craze revamped its marketing efforts to sell to a wider audience. These efforts included a complete redesign of its logo to reflect the recent merger, and improvements to its website meant to capture more information about visitors through the use of cookies.
T-Craze also opened various office locations throughout Europe to help expand its business. While Germany continued to host T-Craze's headquarters and main product-design office, its French affiliate became responsible for all marketing and sales activities. The French affiliate recently procured the services of Right Target, a renowned marketing firm based in the Philippines, to run its latest marketing campaign. After thorough research, Right Target determined that T-Craze is most successful with customers between the ages of 18 and 22. Thus, its first campaign targeted university students in several European capitals, which yielded nearly 40% new customers for T-Craze in one quarter. Right Target also ran subsequent campaigns for T- Craze, though with much less success.
The last two campaigns included a wider demographic group and resulted in countless unsubscribe requests, including a large number in Spain. In fact, the Spanish data protection authority received a complaint from Sofia, a mid-career investment banker. Sofia was upset after receiving a marketing communication even after unsubscribing from such communications from the Right Target on behalf of T-Craze.
Which of the following is T-Craze's lead supervisory authority?
A. France, because that is where T-Craze conducts processing of personal information.
B. Spain, because that is T-Craze's primary market based on its marketing campaigns.
C. Germany, because that is where T-Craze is headquartered.
D. T-Craze may choose its lead supervisory authority where any of its affiliates are based, because it has presence in several European countries.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 39

Under what circumstances might the "soft opt-in" rule apply in relation to direct marketing?
A. When an individual's details are obtained from their inquiries about buying a product.
B. When an individual has not consented to the marketing.
C. Where an individual is given the ability to unsubscribe from marketing emails sent to him.
D. Where an individual's details have been obtained from a bought-in marketing list.
Answer: (SHOW ANSWER)

NEW QUESTION: 40
Which EU institution is vested with the competence to propose new data protection legislation on its own initiative?
A. The European Council
B. The European Commission
C. The Council of the European Union
D. The European Parliament
Answer: C (LEAVE A REPLY)

NEW QUESTION: 41
SCENARIO
Please use the following to answer the next question:
Jason, a long-time customer of ABC insurance, was involved in a minor car accident a few months ago. Although no one was hurt, Jason has been plagued by texts and calls from a company called Erbium Insurance offering to help him recover compensation for personal injury. Jason has heard about insurance companies selling customers' data to third parties, and he's convinced that Erbium must have gotten his information from ABC.
Jason has also been receiving an increased amount of marketing information from ABC, trying to sell him their full range of their insurance policies.
Perturbed by this, Jason has started looking at price comparison sites on the Internet and has been shocked to find that other insurers offer much cheaper rates than ABC, even though he has been a loyal customer for many years. When his ABC policy comes up for renewal, he decides to switch to Xentron Insurance.
In order to activate his new insurance policy, Jason needs to supply Xentron with information about his No Claims bonus, his vehicle and his driving history. After researching his rights under the GDPR, he writes to ask ABC to transfer his information directly to Xentron. He also takes this opportunity to ask ABC to stop using his personal data for marketing purposes.
ABC supplies Jason with a PDF and XML (Extensible Markup Language) versions of his No Claims Certificate, but tells Jason it cannot transfer his data directly to Xentron at this is not technically feasible. ABC also explains that Jason's contract included a provision whereby Jason agreed that his data could be used for marketing purposes; according to ABC, it is too late for Jason to change his mind about this. It angers Jason when he recalls the wording of the contract, which was filled with legal jargon and very confusing.
In the meantime, Jason is still receiving unwanted calls from Erbium Insurance. He writes to Erbium to ask for the name of the organization that supplied his details to them. He warns Erbium that he plans to complain

to the data protection authority because he thinks their company has been using his data unlawfully. His letter states that he does not want his data being used by them in any way.
Erbium's response letter confirms Jason's suspicions. Erbium is ABC's wholly owned subsidiary, and they received information about Jason's accident from ABC shortly after Jason submitted his accident claim. Erbium assures Jason that there has been no breach of the GDPR, as Jason's contract included a provision in which he agreed to share his information with ABC's affiliates for business purposes.
Jason is disgusted by the way in which he has been treated by ABC, and writes to them insisting that all his information be erased from their computer system.
Which statement accurately summarizes ABC's obligation in regard to Jason's data portability request?
A. ABC does not have a duty to transfer Jason's data to Xentron if doing so is legitimately not technically feasible.
B. ABC has failed to comply with the duty to transfer Jason's data to Xentron because the duty applies wherever personal data are processed by automated means and necessary for the performance of a contract with the customer.
C. ABC does not have to transfer Jason's data to Xentron because the right to data portability does not apply where personal data are processed in order to carry out tasks in the public interest.
D. ABC has failed to comply with the duty to transfer Jason's data to Xentron because it has an obligation to develop commonly used, machine-readable and interoperable formats so that all customer data can be ported to other insurers on request.
Answer: (SHOW ANSWER)

NEW QUESTION: 42
Assuming that the "without undue delay" provision is followed, what is the time limit for complying with a data access request?
A. Within 40 days of receipt
B. Within 40 days of receipt, which may be extended by up to 40 additional days
C. Within one month of receipt, which may be extended by up to an additional month
D. Within one month of receipt, which may be extended by an additional two months
Answer: C (LEAVE A REPLY)
Explanation/Reference: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection- regulation-gdpr/individual-rights/right-of-access/

NEW QUESTION: 43
Which area of privacy is a lead supervisory authority's (LSA) MAIN concern?
A. Data subject rights
B. Cross-border processing
C. Special categories of data
D. Data access disputes
Answer: (SHOW ANSWER)

NEW QUESTION: 44

WP29's "Guidelines on Personal data breach notification under Regulation 2016/679" provides examples of ways to communicate data breaches transparently. Which of the following was listed as a method that would NOT be effective for communicating a breach to data subjects?

A. A notice on a corporate blog

B. A postal notification

C. A direct electronic message

D. A prominent advertisement in print media

Answer: A (LEAVE A REPLY)

NEW QUESTION: 45

Please use the following to answer the next question:

WonderkKids provides an online booking service for childcare. Wonderkids is based in France, but hosts its website through a company in Switzerland. As part of their service, WonderKids will pass all personal data provided to them to the childcare provider booked through their system. The type of personal data collected on the website includes the name of the person booking the childcare, address and contact details, as well as information about the children to be cared for including name, age, gender and health information. The privacy statement on Wonderkids' website states the following:

"WonderkKids provides the information you disclose to us through this website to your childcare provider for scheduling and health and safety reasons. We may also use your and your child's personal information for our own legitimate business purposes and we employ a third-party website hosting company located in Switzerland to store the dat a. Any data stored on equipment located in Switzerland meets the European Commission provisions for guaranteeing adequate safeguards for you and your child's personal information. We will only share you and your child's personal information with businesses that we see as adding real value to you. By providing us with any personal data, you consent to its transfer to affiliated businesses and to send you promotional offers."

"We may retain you and your child's personal information for no more than 28 days, at which point the data will be depersonalized, unless your personal information is being used for a legitimate business purpose beyond 28 days where it may be retained for up to 2 years."

"We are processing you and your child's personal information with your consent. If you choose not to provide certain information to us, you may not be able to use our services. You have the right to: request access to you and your child's personal information; rectify or erase you or your child's personal information; the right to correction or erasure of you and/or your child's personal information; object to any processing of you and your child's personal information. You also have the right to complain to the supervisory authority about our data processing activities." What direct marketing information can WonderKids send by email without prior consent of the person booking the childcare?

A. Marketing information related to other business operations of WonderKids.

B. No marketing information at all.

C. Any marketing information at all.

D. Marketing information for products or services similar to those purchased from WonderKids.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 46
What is the key difference between the European Council and the Council of the European Union?
A. The Council of the European Union is helmed by a president.
B. The European Council is comprised of the heads of each EU member state.
Section: (none)
Explanation
C. The Council of the European Union has a degree of legislative power.
D. The European Council focuses primarily on issues involving human rights.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 47
According to the European Data Protection Board, which of the following concepts or practices does NOT follow from the principles relating to the processing of personal data under EU data protection law?
A. Access control management.
B. Error propagation avoidance along the processing chain.
C. Frequent pseudonymization key rotation.
D. Data ownership allocation.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 48
Which statement is correct when considering the right to privacy under Article 8 of the European Convention on Human Rights (ECHR)?
A. The right to privacy has to be balanced against other rights under the ECHR
B. The right to freedom of expression under Article 10 of the ECHR will always override the right to privacy
C. The right to privacy protects the right to hold opinions and to receive and impart ideas without interference
D. The right to privacy is an absolute right
Answer: (SHOW ANSWER)

NEW QUESTION: 49
Under the GDPR, where personal data is not obtained directly from the data subject, a controller is exempt from directly providing information about processing to the data subject if?
A. The data subject already has information regarding how his data will be used
B. The provision of such information to the data subject would be too problematic

C. Third-party data would be disclosed by providing such information to the data subject
D. The processing of the data subject's data is protected by appropriate technical measures
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://dataprivacymanager.net/gdpr-exemptions-from-the-obligation-to-provide-information-to-the- individual-data-subject/

NEW QUESTION: 50
SCENARIO
Please use the following to answer the next question:
Jason, a long-time customer of ABC insurance, was involved in a minor car accident a few months ago. Although no one was hurt, Jason has been plagued by texts and calls from a company called Erbium Insurance offering to help him recover compensation for personal injury. Jason has heard about insurance companies selling customers' data to third parties, and he's convinced that Erbium must have gotten his information from ABC.
Jason has also been receiving an increased amount of marketing information from ABC, trying to sell him their full range of their insurance policies.
Perturbed by this, Jason has started looking at price comparison sites on the Internet and has been shocked to find that other insurers offer much cheaper rates than ABC, even though he has been a loyal customer for many years. When his ABC policy comes up for renewal, he decides to switch to Xentron Insurance.
In order to activate his new insurance policy, Jason needs to supply Xentron with information about his No Claims bonus, his vehicle and his driving history. After researching his rights under the GDPR, he writes to ask ABC to transfer his information directly to Xentron. He also takes this opportunity to ask ABC to stop using his personal data for marketing purposes.
ABC supplies Jason with a PDF and XML (Extensible Markup Language) versions of his No Claims Certificate, but tells Jason it cannot transfer his data directly to Xentron at this is not technically feasible. ABC also explains that Jason's contract included a provision whereby Jason agreed that his data could be used for marketing purposes; according to ABC, it is too late for Jason to change his mind about this. It angers Jason when he recalls the wording of the contract, which was filled with legal jargon and very confusing.
In the meantime, Jason is still receiving unwanted calls from Erbium Insurance. He writes to Erbium to ask for the name of the organization that supplied his details to them. He warns Erbium that he plans to complain to the data protection authority because he thinks their company has been using his data unlawfully. His letter states that he does not want his data being used by them in any way.
Erbium's response letter confirms Jason's suspicions. Erbium is ABC's wholly owned subsidiary, and they received information about Jason's accident from ABC shortly after Jason submitted his accident claim. Erbium assures Jason that there has been no breach of the GDPR, as Jason's contract included a provision in which he agreed to share his information with ABC's affiliates for business purposes.
Jason is disgusted by the way in which he has been treated by ABC, and writes to them insisting that all his information be erased from their computer system.
After Jason has exercised his right to restrict the use of his data, under what conditions would Erbium have grounds for refusing to comply?
A. If the accuracy of the data is not an aspect that Jason is disputing.

B. If Erbium also uses the data to conduct public health research.
C. If the data becomes necessary to defend Erbium's legal rights.
D. If Erbium is entitled to use of the data as an affiliate of ABC.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 51
SCENARIO
Please use the following to answer the next question:
Zandelay Fashion ('Zandelay') is a successful international online clothing retailer that employs approximately 650 people at its headquarters based in Dublin, Ireland. Martin is their recently appointed data protection officer, who oversees the company's compliance with the General Data Protection Regulation (GDPR) and other privacy legislation.
The company offers both male and female clothing lines across all age demographics, including children. In doing so, the company processes large amounts of information about such customers, including preferences and sensitive financial information such as credit card and bank account numbers.
In an aggressive bid to build revenue growth, Jerry, the CEO, tells Martin that the company is launching a new mobile app and loyalty scheme that puts significant emphasis on profiling the company's customers by analyzing their purchases. Martin tells the CEO that: (a) the potential risks of such activities means that Zandelay needs to carry out a data protection impact assessment to assess this new venture and its privacy implications; and (b) where the results of this assessment indicate a high risk in the absence of appropriate protection measures. Zandelay may have to undertake a prior consultation with the Irish Data Protection Commissioner before implementing the app and loyalty scheme.
Jerry tells Martin that he is not happy about the prospect of having to directly engage with a supervisory authority and having to disclose details of Zandelay's business plan and associated processing activities.
What must Zandelay provide to the supervisory authority during the prior consultation?
A. An evaluation of the complexity of the intended processing.
B. An explanation of the purposes and means of the intended processing.
C. Certificates that prove Martin's professional qualities and expert knowledge of data protection law.
D. Records showing that customers have explicitly consented to the intended profiling activities.
Answer: (SHOW ANSWER)

NEW QUESTION: 52
SCENARIO
Please use the following to answer the next question:
ABC Hotel Chain and XYZ Travel Agency are U.S.-based multinational companies. They use an internet-based common platform for collecting and sharing their customer data with each other, in order to integrate their marketing efforts. Additionally, they agree on the data to be stored, how reservations will be booked and confirmed, and who has access to the stored data.
Mike, an EU resident, has booked travel itineraries in the past through XYZ Travel Agency to stay at ABC Hotel Chain's locations. XYZ Travel Agency offers a rewards program that allows customers to sign up to

accumulate points that can later be redeemed for free travel. Mike has signed the agreement to be a rewards program member.
Now Mike wants to know what personal information the company holds about him. He sends an email requesting access to his data, in order to exercise what he believes are his data subject rights.
What is the time period in which Mike should receive a response to his request?
A. Not more than two months after verifying Mike's identity.
B. Not more than one month of receipt of Mike's request.
C. When all the information about Mike has been collected.
D. Not more than thirty days after submission of Mike's request.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 53
SCENARIO
Please use the following to answer the next question:
Javier is a member of the fitness club EVERFIT. This company has branches in many EU member states, but for the purposes of the GDPR maintains its primary establishment in France. Javier lives in Newry, Northern Ireland (part of the U.K.), and commutes across the border to work in Dundalk, Ireland. Two years ago while on a business trip, Javier was photographed while working out at a branch of EVERFIT in Frankfurt, Germany. At the time, Javier gave his consent to being included in the photograph, since he was told that it would be used for promotional purposes only. Since then, the photograph has been used in the club's U.K. brochures, and it features in the landing page of its U.K. website. However, the fitness club has recently fallen into disrepute due to widespread mistreatment of members at various branches of the club in several EU member states. As a result, Javier no longer feels comfortable with his photograph being publicly associated with the fitness club.
After numerous failed attempts to book an appointment with the manager of the local branch to discuss this matter, Javier sends a letter to EVETFIT requesting that his image be removed from the website and all promotional materials. Months pass and Javier, having received no acknowledgment of his request, becomes very anxious about this matter. After repeatedly failing to contact EVETFIT through alternate channels, he decides to take action against the company.
Javier contacts the U.K. Information Commissioner's Office ('ICO' - the U.K.'s supervisory authority) to lodge a complaint about this matter. The ICO, pursuant to Article 56 (3) of the GDPR, informs the CNIL (i.e. the supervisory authority of EVERFIT's main establishment) about this matter. Despite the fact that EVERFIT has an establishment in the U.K., the CNIL decides to handle the case in accordance with Article 60 of the GDPR.
The CNIL liaises with the ICO, as relevant under the cooperation procedure. In light of issues amongst the supervisory authorities to reach a decision, the European Data Protection Board becomes involved and, pursuant to the consistency mechanism, issues a binding decision.
Additionally, Javier sues EVERFIT for the damages caused as a result of its failure to honor his request to have his photograph removed from the brochure and website.
Under the cooperation mechanism, what should the lead authority (the CNIL) do after it has formed its view on the matter?

A. Submit a draft decision to other supervisory authorities for their opinion.
B. Request that members of the seconding supervisory authority and the host supervisory authority co-draft a decision.
C. Submit a draft decision directly to the Commission to ensure the effectiveness of the consistency mechanism.
D. Request that the other supervisory authorities provide the lead authority with a draft decision for its consideration.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 54
Which type of personal data does the GDPR define as a "special category" of personal data?
A. Closed Circuit Television (CCTV) footage.
B. Trade-union membership.
C. Financial information.
D. Educational history.
Answer: (SHOW ANSWER)

NEW QUESTION: 55
Which of the following demonstrates compliance with the accountability principle found in Article 5, Section 2 of the GDPR?
A. Anonymizing special categories of data.
B. Conducting regular audits of the data protection program.
C. Encrypting data in transit and at rest using strong encryption algorithms.
D. Getting consent from the data subject for a cross border data transfer.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 56
Which of the following is an example of direct marketing that would be subject to European data protection laws?
A. A charity fundraising event notice sent to an individual at her business address.
B. An updated privacy notice sent to an individual's personal email address.
C. A revision of contract terms conveyed to an individual by SMS from a marketing organization.
D. A service outage notification provided to an individual by recorded telephone message.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 57
When does the European Data Protection Board (EDPB) recommend reevaluating whether a transfer tool is effectively providing a level of personal data protection that is in compliance with the European Union (EU) level?
A. Every three (3) years.
B. Every year.

C. On an ongoing basis.
D. After a personal data breach.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 58
A company is located in a country NOT considered by the European Union (EU) to have an adequate level of data protection. Which of the following is an obligation of the company if it imports personal data from another organization in the European Economic Area (EEA) under standard contractual clauses?
A. Ensure that notice is given to and consent is obtained from data subjects.
B. Supply any information requested by a data protection authority (DPA) within 30 days.
C. Submit the contract to its own government authority.
D. Ensure that local laws do not impede the company from meeting its contractual obligations.
Answer: (SHOW ANSWER)

NEW QUESTION: 59
Which of the following would most likely NOT be covered by the definition of "personal data" under the GDPR?
A. The U.S. social security number of an American citizen living in France
B. The identification number of a German candidate for a professional examination in Germany
C. The unlinked aggregated data used for statistical purposes by an Italian company
D. The payment card number of a Dutch citizen
Answer: (SHOW ANSWER)

NEW QUESTION: 60
Under which of the following conditions does the General Data Protection Regulation NOT apply to the processing of personal data?
A. When the personal data is processed only in non-electronic form
B. When the personal data is processed by an individual only for their household activities
C. When the personal data is held by the controller but not processed for further purposes
D. When the personal data is collected and then pseudonymised by the controller
Answer: D (LEAVE A REPLY)

NEW QUESTION: 61
Under the GDPR, which essential pieces of information must be provided to data subjects before collecting their personal data?
A. The contact information of the controller and a description of the retention policy.
B. The name/s of relevant government agencies involved and the steps needed for revising the data.
C. The identity and contact details of the controller and the reasons the data is being collected.
D. The authority by which the controller is collecting the data and the third parties to whom the data will be sent.
Answer: (SHOW ANSWER)

NEW QUESTION: 62
SCENARIO
Please use the following to answer the next question:
Liem, an online retailer known for its environmentally friendly shoes, has recently expanded its presence in Europe. Anxious to achieve market dominance, Liem teamed up with another eco friendly company, EcoMick, which sells accessories like belts and bags. Together the companies drew up a series of marketing campaigns designed to highlight the environmental and economic benefits of their products. After months of planning, Liem and EcoMick entered into a data sharing agreement to use the same marketing database, MarketIQ, to send the campaigns to their respective contacts.
Liem and EcoMick also entered into a data processing agreement with MarketIQ, the terms of which included processing personal data only upon Liem and EcoMick's instructions, and making available to them all information necessary to demonstrate compliance with GDPR obligations.
Liem and EcoMick then procured the services of a company called JaphSoft, a marketing optimization firm that uses machine learning to help companies run successful campaigns. Clients provide JaphSoft with the personal data of individuals they would like to be targeted in each campaign. To ensure protection of its clients' data, JaphSoft implements the technical and organizational measures it deems appropriate. JaphSoft works to continually improve its machine learning models by analyzing the data it receives from its clients to determine the most successful components of a successful campaign. JaphSoft then uses such models in providing services to its client-base. Since the models improve only over a period of time as more information is collected, JaphSoft does not have a deletion process for the data it receives from clients. However, to ensure compliance with data privacy rules, JaphSoft pseudonymizes the personal data by removing identifying information from the contact information. JaphSoft's engineers, however, maintain all contact information in the same database as the identifying information.
Under its agreement with Liem and EcoMick, JaphSoft received access to MarketIQ, which included contact information as well as prior purchase history for such contacts, to create campaigns that would result in the most views of the two companies' websites. A prior Liem customer, Ms. Iman, received a marketing campaign from JaphSoft regarding Liem's as well as EcoMick's latest products. While Ms. Iman recalls checking a box to receive information in the future regarding Liem's products, she has never shopped EcoMick, nor provided her personal data to that company.
Why would the consent provided by Ms. Iman NOT be considered valid in regard to JaphSoft?
A. She was not told which controller would be processing her personal data.
B. She only viewed the visual representations of the privacy notice Liem provided.

C. She has never made any purchases from JaphSoft and has no relationship with the company.
D. She did not read the privacy notice stating that her personal data would be shared.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 63
Which sentence BEST summarizes the concepts of "fairness," "lawfulness" and "transparency", as expressly required by Article 5 of the GDPR?
A. Fairness and transparency refer to the communication of key information before collecting data; lawfulness refers to compliance with government regulations.
B. Fairness refers to limiting the amount of data collected from individuals; lawfulness refers to the approval of company guidelines by the state; transparency solely relates to communication of key information before collecting data.
C. Fairness refers to the security of personal data; lawfulness and transparency refers to the analysis of ordinances to ensure they are uniformly enforced.
D. Fairness refers to the collection of data from diverse subjects; lawfulness refers to the need for legal rules to be uniform; transparency refers to giving individuals access to their data.
Answer: A (LEAVE A REPLY)
Explanation

NEW QUESTION: 64
Which of the following was the first to implement national law for data protection in 1973?
A. France
B. Sweden
C. United Kingdom
D. Germany
Answer: (SHOW ANSWER)

NEW QUESTION: 65
SCENARIO
Please use the following to answer the next question:
TripBliss Inc. is a travel service company which has lost substantial revenue over the last few years. Their new manager, Oliver, suspects that this is partly due to the company's outdated website. After doing some research, he meets with a sales representative from the up-and-coming IT company Techiva, hoping that they can design a new, cutting-edge website for TripBliss Inc.'s foundering business.
During negotiations, a Techiva representative describes a plan for gathering more customer information through detailed Questionaires, which could be used to tailor their preferences to specific travel destinations. TripBliss Inc. can choose any number of data categories - age, income, ethnicity - that would help them best accomplish their goals. Oliver loves this idea, but would also like to have some way of gauging how successful this approach is, especially since the Questionaires will require customers to provide explicit consent to having their data collected. The Techiva representative suggests that they also run a program to analyze the new website's traffic, in order to get a better understanding of how customers are using it. He

explains his plan to place a number of cookies on customer devices. The cookies will allow the company to collect IP addresses and other information, such as the sites from which the customers came, how much time they spend on the TripBliss Inc. website, and which pages on the site they visit. All of this information will be compiled in log files, which Techiva will analyze by means of a special program. TripBliss Inc. would receive aggregate statistics to help them evaluate the website's effectiveness. Oliver enthusiastically engages Techiva for these services.
Techiva assigns the analytics portion of the project to longtime account manager Leon Santos. As is standard practice, Leon is given administrator rights to TripBliss Inc.'s website, and can authorize access to the log files gathered from it. Unfortunately for TripBliss Inc., however, Leon is taking on this new project at a time when his dissatisfaction with Techiva is at a high point. In order to take revenge for what he feels has been unfair treatment at the hands of the company, Leon asks his friend Fred, a hobby hacker, for help. Together they come up with the following plan: Fred will hack into Techiva's system and copy their log files onto a USB stick. Despite his initial intention to send the USB to the press and to the data protection authority in order to denounce Techiva, Leon experiences a crisis of conscience and ends up reconsidering his plan. He decides instead to securely wipe all the data from the USB stick and inform his manager that the company's system of access control must be reconsidered.
If TripBliss Inc. decides not to report the incident to the supervisory authority, what would be their BEST defense?
A. The incident resulted from the actions of a third-party that were beyond their control.
B. The sensitivity of the categories of data involved in the incident was not substantial enough.
C. The resulting obligation to notify data subjects would involve disproportionate effort.
D. The destruction of the stolen data makes any risk to the affected data subjects unlikely.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 66
Under the GDPR, which of the following is true in regard to adequacy decisions involving cross-border transfers?
A. The European Commission can adopt an adequacy decision for individual companies.
B. The European Commission can adopt, repeal or amend an existing adequacy decision.
C. EU member states are vested with the power to accept or reject a European Commission adequacy decision.
D. To be considered as adequate, third countries must implement the EU General Data Protection Regulation into their national legislation.
Answer: A (LEAVE A REPLY)
Explanation/Reference: https://www.futurelearn.com/courses/general-data-protection-regulation/0/steps/32449

NEW QUESTION: 67
An unforeseen power outage results in company Z's lack of access to customer data for six hours. According to article 32 of the GDPR, this is considered a breach. Based on the WP 29's February, 2018 guidance, company Z should do which of the following?

A. Conduct a thorough audit of all security systems
B. Notify the supervisory authority about the loss of availability
C. Document the loss of availability to demonstrate accountability
D. Notify affected individuals that their data was unavailable for a period of time.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 68
SCENARIO
Please use the following to answer the next question:
WonderkKids provides an online booking service for childcare. Wonderkids is based in France, but hosts its website through a company in Switzerland. As part of their service, WonderKids will pass all personal data provided to them to the childcare provider booked through their system. The type of personal data collected on the website includes the name of the person booking the childcare, address and contact details, as well as information about the children to be cared for including name, age, gender and health information. The privacy statement on Wonderkids' website states the following:
"WonderkKids provides the information you disclose to us through this website to your childcare provider for scheduling and health and safety reasons. We may also use your and your child's personal information for our own legitimate business purposes and we employ a third-party website hosting company located in Switzerland to store the dat a. Any data stored on equipment located in Switzerland meets the European Commission provisions for guaranteeing adequate safeguards for you and your child's personal information. We will only share you and your child's personal information with businesses that we see as adding real value to you. By providing us with any personal data, you consent to its transfer to affiliated businesses and to send you promotional offers."
"We may retain you and your child's personal information for no more than 28 days, at which point the data will be depersonalized, unless your personal information is being used for a legitimate business purpose beyond 28 days where it may be retained for up to 2 years."
"We are processing you and your child's personal information with your consent. If you choose not to provide certain information to us, you may not be able to use our services. You have the right to: request access to you and your child's personal information; rectify or erase you or your child's personal information; the right to correction or erasure of you and/or your child's personal information; object to any processing of you and your child's personal information. You also have the right to complain to the supervisory authority about our data processing activities." What additional information must Wonderkids provide in their Privacy Statement?
A. Technical and organizational measures to protect data.
B. The categories of recipients with whom data will be shared.
C. How often promotional emails will be sent.
D. Contact information of the hosting company.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 69
In which of the following situations would an individual most likely to be able to withdraw her consent for processing?

A. When she has recently changed jobs and no longer works for the same company.
B. When she disagrees with a diagnosis her doctor has recorded on her records.
C. When she is leaving her bank and moving to another bank.
D. When she no longer wishes to be sent marketing materials from an organization.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 70
Under the Data Protection Law Enforcement Directive of the EU, a government can carry out covert investigations involving personal data, as long it is set forth by law and constitutes a measure that is both necessary and what?
A. DPA-approved.
B. Proportionate.
C. Important.
D. Prudent.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 71
A well-known video production company, based in Spain but specializing in documentaries filmed worldwide, has just finished recording several hours of footage featuring senior citizens in the streets of Madrid. Under what condition would the company NOT be required to obtain the consent of everyone whose image they use for their documentary?
A. If obtaining consent is deemed to involve disproportionate effort.
B. If obtaining consent is deemed voluntary by local legislation.
C. If the company limits the footage to data subjects solely of legal age.
D. If the company's status as a documentary provider allows it to claim legitimate interest.
Answer: B (LEAVE A REPLY)
Explanation

NEW QUESTION: 72
SCENARIO
Please use the following to answer the next question:
Javier is a member of the fitness club EVERFIT. This company has branches in many EU member states, but for the purposes of the GDPR maintains its primary establishment in France. Javier lives in Newry, Northern Ireland (part of the U.K.), and commutes across the border to work in Dundalk, Ireland. Two years ago while on a business trip, Javier was photographed while working out at a branch of EVERFIT in Frankfurt, Germany. At the time, Javier gave his consent to being included in the photograph, since he was told that it would be used for promotional purposes only. Since then, the photograph has been used in the club's U.K. brochures, and it features in the landing page of its U.K. website. However, the fitness club has recently fallen into disrepute due to widespread mistreatment of members at various branches of the club in several EU member states. As a result, Javier no longer feels comfortable with his photograph being publicly associated with the fitness club.

After numerous failed attempts to book an appointment with the manager of the local branch to discuss this matter, Javier sends a letter to EVETFIT requesting that his image be removed from the website and all promotional materials. Months pass and Javier, having received no acknowledgment of his request, becomes very anxious about this matter. After repeatedly failing to contact EVETFIT through alternate channels, he decides to take action against the company.
Javier contacts the U.K. Information Commissioner's Office ('ICO' - the U.K.'s supervisory authority) to lodge a complaint about this matter. The ICO, pursuant to Article 56 (3) of the GDPR, informs the CNIL (i.e. the supervisory authority of EVERFIT's main establishment) about this matter. Despite the fact that EVERFIT has an establishment in the U.K., the CNIL decides to handle the case in accordance with Article 60 of the GDPR. The CNIL liaises with the ICO, as relevant under the cooperation procedure. In light of issues amongst the supervisory authorities to reach a decision, the European Data Protection Board becomes involved and, pursuant to the consistency mechanism, issues a binding decision.
Additionally, Javier sues EVERFIT for the damages caused as a result of its failure to honor his request to have his photograph removed from the brochure and website.
Assuming that multiple EVETFIT branches across several EU countries are acting as separate data controllers, and that each of those branches were responsible for mishandling Javier's request, how may Javier proceed in order to seek compensation?
A. He will have to sue the EVETFIT's head office in France, where EVETFIT has its main establishment.
B. He will have to sue each EVETFIT branch so that each branch provides proportionate compensation commensurate with its contribution to the damage or distress suffered by Javier.
C. He will be able to sue any one of the relevant EVETFIT branches, as each one may be held liable for the entire damage.
D. He will be able to apply to the European Data Protection Board in order to determine which particular EVETFIT branch is liable for damages, based on the decision that was made by the board.
Answer: (SHOW ANSWER)

NEW QUESTION: 73
Under Article 21 of the GDPR, a controller must stop profiling when requested by a data subject, unless it can demonstrate compelling legitimate grounds that override the interests of the individual. In the Guidelines on Automated individual decision-making and Profiling, the WP 29 says the controller needs to do all of the following to demonstrate that it has such legitimate grounds EXCEPT?
A. Carry out an exercise that weighs the interests of the controller and the basis for the data subject's objection.
B. Consider the impact of the profiling on the data subject's interest, rights and freedoms.
C. Demonstrate that the profiling is for the purposes of direct marketing.
D. Consider the importance of the profiling to their particular objective.
Answer: C (LEAVE A REPLY)
Explanation/Reference: https://gdpr-info.eu/art-21-gdpr/

NEW QUESTION: 74

In 2016's Guidance, the United Kingdom's Information Commissioner's Office (ICO) reaffirmed the importance of using a "layered notice" to provide data subjects with what?

A. An efficient means of providing written consent in member states where they are required to do so.

B. A privacy notice containing brief information whilst offering access to further detail.

C. A privacy notice explaining the consequences for opting out of the use of cookies on a website.

D. An explanation of the security measures used when personal data is transferred to a third party.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 75

An unforeseen power outage results in company Z's lack of access to customer data for six hours. According to article 32 of the GDPR, this is considered a breach. Based on the WP 29's February, 2018 guidance, company Z should do which of the following?

A. Notify affected individuals that their data was unavailable for a period of time.

B. Document the loss of availability to demonstrate accountability

C. Notify the supervisory authority about the loss of availability

D. Conduct a thorough audit of all security systems

Answer: C (LEAVE A REPLY)

Explanation/Reference: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwihmsidxtTqAhXvQUEAHXRaAdYQFjABegQIARAB&url=https%3A%2F%2Fec.europa.eu%2Fnewsroom%2Farticle29%2Fdocument.cfm%3Fdoc_id%3D49827&usg=AOvVaw2uhYsKyRzJ6lwhQyiMURJF (5)

NEW QUESTION: 76

SCENARIO

Please use the following to answer the next question:

Brady is a computer programmer based in New Zealand who has been running his own business for two years. Brady's business provides a low-cost suite of services to customers throughout the European Economic Area (EEA). The services are targeted towards new and aspiring small business owners. Brady's company, called Brady Box, provides web page design services, a Social Networking Service (SNS) and consulting services that help people manage their own online stores.

Unfortunately, Brady has been receiving some complaints. A customer named Anna recently uploaded her plans for a new product onto Brady Box's chat area, which is open to public viewing. Although she realized her mistake two weeks later and removed the document, Anna is holding Brady Box responsible for not noticing the error through regular monitoring of the website. Brady believes he should not be held liable.

Another customer, Felipe, was alarmed to discover that his personal information was transferred to a third-party contractor called Hermes Designs and worries that sensitive information regarding his business plans may be misused. Brady does not believe he violated European privacy rules. He provides a privacy notice to all of his customers explicitly stating that personal data may be transferred to specific third parties in fulfillment of a requested service. Felipe says he read the privacy notice but that it was long and complicated Brady continues to insist that Felipe has no need to be concerned, as he can personally vouch for the integrity of Hermes Designs. In fact, Hermes Designs has taken the initiative to create sample customized

banner advertisements for customers like Felipe. Brady is happy to provide a link to the example banner ads, now posted on the Hermes Designs webpage. Hermes Designs plans on following up with direct marketing to these customers.
Brady was surprised when another customer, Serge, expressed his dismay that a quotation by him is being used within a graphic collage on Brady Box's home webpage. The quotation is attributed to Serge by first and last name. Brady, however, was not worried about any sort of litigation. He wrote back to Serge to let him know that he found the quotation within Brady Box's Social Networking Service (SNS), as Serge himself had posted the quotation. In his response, Brady did offer to remove the quotation as a courtesy.
Despite some customer complaints, Brady's business is flourishing. He even supplements his income through online behavioral advertising (OBA) via a third-party ad network with whom he has set clearly defined roles. Brady is pleased that, although some customers are not explicitly aware of the OBA, the advertisements contain useful products and services.
Based on current trends in European privacy practices, which aspect of Brady Box' Online Behavioral Advertising (OBA) is most likely to be insufficient if the company becomes established in Europe?
A. The lack of the option to opt in.
B. The level of security within the website.
C. The contract with the third-party advertising network.
D. The need to have the contents of the advertising approved.
Answer: A (LEAVE A REPLY)
Section: (none)
Explanation

NEW QUESTION: 77
SCENARIO
Please use the following to answer the next question:
Joe is the new privacy manager for Who-R-U, a Canadian business that provides DNA analysis. The company is headquartered in Montreal, and all of its employees are located there. The company offers its services to Canadians only: Its website is in English and French, it accepts only Canadian currency, and it blocks internet traffic from outside of Canada (although this solution doesn't prevent all non-Canadian traffic). It also declines to process orders that request the DNA report to be sent outside of Canada, and returns orders that show a non-Canadian return address.
Bob, the President of Who-R-U, thinks there is a lot of interest for the product in the EU, and the company is exploring a number of plans to expand its customer base.

The first plan, collegially called We-Track-U, will use an app to collect information about its current Canadian customer base. The expansion will allow its Canadian customers to use the app while traveling abroad. He suggests that the company use this app to gather location information. If the plan shows promise, Bob proposes to use push notifications and text messages to encourage existing customers to pre-register for an EU version of the service. Bob calls this work plan, We-Text-U. Once the company has gathered enough pre-registrations, it will develop EU-specific content and services.
Another plan is called Customer for Life. The idea is to offer additional services through the company's app, like storage and sharing of DNA information with other applications and medical providers. The company's contract says that it can keep customer DNA indefinitely, and use it to offer new services and market them to customers. It also says that customers agree not to withdraw direct marketing consent. Paul, the marketing director, suggests that the company should fully exploit these provisions, and that it can work around customers' attempts to withdraw consent because the contract invalidates them.
The final plan is to develop a brand presence in the EU. The company has already begun this process. It is in the process of purchasing the naming rights for a building in Germany, which would come with a few offices that Who-R-U executives can use while traveling internationally. The office doesn't include any technology or infrastructure; rather, it's simply a room with a desk and some chairs.
On a recent trip concerning the naming-rights deal, Bob's laptop is stolen. The laptop held unencrypted DNA reports on 5,000 Who-R-U customers, all of whom are residents of Canad a. The reports include customer name, birthdate, ethnicity, racial background, names of relatives, gender, and occasionally health information.
The Customer for Life plan may conflict with which GDPR provision?
A. Article 7, which requires consent to be as easy to withdraw as it is to give.
B. Article 20, which gives data subjects a right to data portability.
C. Article 6, which requires processing to be lawful.
D. Article 16, which provides data subjects with a rights to rectification.
Answer: (SHOW ANSWER)

NEW QUESTION: 78
SCENARIO
Please use the following to answer the next question:
You have just been hired by a toy manufacturer based in Hong Kong. The company sells a broad range of dolls, action figures and plush toys that can be found internationally in a wide variety of retail stores. Although the manufacturer has no offices outside Hong Kong and in fact does not employ any staff outside Hong Kong, it has entered into a number of local distribution contracts. The toys produced by the company can be found in all popular toy stores throughout Europe, the United States and Asia. A large portion of the company's revenue is due to international sales.
The company now wishes to launch a new range of connected toys, ones that can talk and interact with children. The CEO of the company is touting these toys as the next big thing, due to the increased possibilities offered: The figures can answer children's questions on various subjects, such as mathematical calculations or the weather. Each figure is equipped with a microphone and speaker and can connect to any smartphone or tablet via Bluetooth. Any mobile device within a 10-meter radius can connect to the toys via

Bluetooth as well. The figures can also be associated with other figures (from the same manufacturer) and interact with each other for an enhanced play experience.
When a child asks the toy a question, the request is sent to the cloud for analysis, and the answer is generated on cloud servers and sent back to the figure. The answer is given through the figure's integrated speakers, making it appear as though that the toy is actually responding to the child's question. The packaging of the toy does not provide technical details on how this works, nor does it mention that this feature requires an internet connection. The necessary data processing for this has been outsourced to a data center located in South Africa. However, your company has not yet revised its consumer-facing privacy policy to indicate this.
In parallel, the company is planning to introduce a new range of game systems through which consumers can play the characters they acquire in the course of playing the game. The system will come bundled with a portal that includes a Near-Field Communications (NFC) reader. This device will read an RFID tag in the action figure, making the figure come to life onscreen. Each character has its own stock features and abilities, but it is also possible to earn additional ones by accomplishing game goals. The only information stored in the tag relates to the figures' abilities. It is easy to switch characters during the game, and it is possible to bring the figure to locations outside of the home and have the character's abilities remain intact.
To ensure GDPR compliance, what should be the company's position on the issue of consent?
A. Parental consent for a child's use of the action figures would have to be obtained before any data could be collected.
B. Consent for data collection is implied through the parent's purchase of the action figure for the child.
C. The child, as the user of the action figure, can provide consent himself, as long as no information is shared for marketing purposes.
D. Written authorization attesting to the responsible use of children's data would need to be obtained from the supervisory authority.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 79
A worker in a European Union (EU) member state has ceased his employment with a company. What should the employer most likely do in regard to the worker's personal data?
A. Store all of the data in case the departing worker makes a subject access request.
B. Destroy sensitive information and store the rest per applicable data protection rules.
C. Provide the employee the reasons for retaining the data.
D. Securely store the data that is required to be kept under local law.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 80
With respect to international transfers of personal data, the European Data Protection Board (EDPB) confirmed that derogations may be relied upon under what condition?
A. When it has been determined that adequate protection can be performed.
B. Only as a last resort and when interpreted restrictively.

C. If the data controller has received preapproval from a Data Protection Authority (DPA), after submitting the appropriate documents.
D. Only if the Data Protection Impact Assessment (DPIA) shows low risk.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 81
Which of the following would require designating a data protection officer?
A. Processing is carried out for the purpose of providing for-profit goods or services to individuals in the EU.
B. The core activities of the controller or processor consist of processing operations of financial information or information relating to children.
C. Processing is carried out by an organization employing 250 persons or more.
D. The core activities of the controller or processor consist of processing operations that require systematic monitoring of data subjects on a large scale.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 82
To receive a preliminary interpretation on provisions of the GDPR, a national court will refer its case to which of the following?
A. The European Court of Human Rights.
B. The European Data Protection Supervisor.
C. The European Data Protection Board.
D. The Court of Justice of the European Union.
Answer: (SHOW ANSWER)

NEW QUESTION: 83
Under the GDPR, who would be LEAST likely to be allowed to engage in the collection, use, and disclosure of a data subject's sensitive medical information without the data subject's knowledge or consent?
A. A public authority responsible for public health, where the sharing of such information is considered necessary for the protection of the general populace.
B. A member of the judiciary involved in adjudicating a legal dispute involving the data subject and concerning the health of the data subject.
C. A journalist writing an article relating to the medical condition in question, who believes that the publication of such information is in the public interest.
D. A health professional involved in the medical care for the data subject, where the data subject's life hinges on the timely dissemination of such information.
Answer: (SHOW ANSWER)

NEW QUESTION: 84
SCENARIO
Please use the following to answer the next question:

You have just been hired by a toy manufacturer based in Hong Kong. The company sells a broad range of dolls, action figures and plush toys that can be found internationally in a wide variety of retail stores. Although the manufacturer has no offices outside Hong Kong and in fact does not employ any staff outside Hong Kong, it has entered into a number of local distribution contracts. The toys produced by the company can be found in all popular toy stores throughout Europe, the United States and Asia. A large portion of the company's revenue is due to international sales.

The company now wishes to launch a new range of connected toys, ones that can talk and interact with children. The CEO of the company is touting these toys as the next big thing, due to the increased possibilities offered: The figures can answer children's questions on various subjects, such as mathematical calculations or the weather. Each figure is equipped with a microphone and speaker and can connect to any smartphone or tablet via Bluetooth. Any mobile device within a 10-meter radius can connect to the toys via Bluetooth as well.

The figures can also be associated with other figures (from the same manufacturer) and interact with each other for an enhanced play experience.

When a child asks the toy a question, the request is sent to the cloud for analysis, and the answer is generated on cloud servers and sent back to the figure. The answer is given through the figure's integrated speakers, making it appear as though that the toy is actually responding to the child's question. The packaging of the toy does not provide technical details on how this works, nor does it mention that this feature requires an internet connection. The necessary data processing for this has been outsourced to a data center located in South Africa. However, your company has not yet revised its consumer-facing privacy policy to indicate this.

In parallel, the company is planning to introduce a new range of game systems through which consumers can play the characters they acquire in the course of playing the game. The system will come bundled with a portal that includes a Near-Field Communications (NFC) reader. This device will read an RFID tag in the action figure, making the figure come to life onscreen. Each character has its own stock features and abilities, but it is also possible to earn additional ones by accomplishing game goals. The only information stored in the tag relates to the figures' abilities. It is easy to switch characters during the game, and it is possible to bring the figure to locations outside of the home and have the character's abilities remain intact.

To ensure GDPR compliance, what should be the company's position on the issue of consent?

A. Written authorization attesting to the responsible use of children's data would need to be obtained from the supervisory authority.

B. Consent for data collection is implied through the parent's purchase of the action figure for the child.

C. Parental consent for a child's use of the action figures would have to be obtained before any data could be collected.

D. The child, as the user of the action figure, can provide consent himself, as long as no information is shared for marketing purposes.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 85

SCENARIO

Please use the following to answer the next question:

Louis, a long-time customer of Bedrock Insurance, was involved in a minor car accident a few months ago. Although no one was hurt, Louis has been plagued by texts and calls from a company called Accidentable offering to help him recover compensation for personal injury. Louis has heard about insurance companies selling customers' data to third parties, and he's convinced that Accidentable must have gotten his information from Bedrock Insurance.

Louis has also been receiving an increased amount of marketing information from Bedrock, trying to sell him their full range of their insurance policies.

Perturbed by this, Louis has started looking at price comparison sites on the internet and has been shocked to find that other insurers offer much cheaper rates than Bedrock, even though he has been a loyal customer for many years. When his Bedrock policy comes up for renewal, he decides to switch to Zantrum Insurance.

In order to activate his new insurance policy, Louis needs to supply Zantrum with information about his No Claims bonus, his vehicle and his driving history. After researching his rights under the GDPR, he writes to ask Bedrock to transfer his information directly to Zantrum. He also takes this opportunity to ask Bedrock to stop using his personal data for marketing purposes.

Bedrock supplies Louis with a PDF and XML (Extensible Markup Language) versions of his No Claims Certificate, but tells Louis it cannot transfer his data directly to Zantrum as this is not technically feasible. Bedrock also explains that Louis's contract included a provision whereby Louis agreed that his data could be used for marketing purposes; according to Bedrock, it is too late for Louis to change his mind about this. It angers Louis when he recalls the wording of the contract, which was filled with legal jargon and very confusing.

In the meantime, Louis is still receiving unwanted calls from Accidentable Insurance. He writes to Accidentable to ask for the name of the organization that supplied his details to them. He warns Accidentable that he plans to complain to the data protection authority, because he thinks their company has been using his data unlawfully. His letter states that he does not want his data being used by them in any way.

Accidentable's response letter confirms Louis's suspicions. Accidentable is Bedrock Insurance's wholly owned subsidiary, and they received information about Louis's accident from Bedrock shortly after Louis submitted his accident claim. Accidentable assures Louis that there has been no breach of the GDPR, as Louis's contract included, a provision in which he agreed to share his information with Bedrock's affiliates for business purposes.

Louis is disgusted by the way in which he has been treated by Bedrock, and writes to them insisting that all his information be erased from their computer system.

After Louis has exercised his right to restrict the use of his data, under what conditions would Accidentable have grounds for refusing to comply?

A. If Accidentable is entitled to use of the data as an affiliate of Bedrock.

B. If Accidentable also uses the data to conduct public health research.

C. If the data becomes necessary to defend Accidentable's legal rights.

D. If the accuracy of the data is not an aspect that Louis is disputing.

Answer: (SHOW ANSWER)

Explanation/Reference:

NEW QUESTION: 86

SCENARIO
Please use the following to answer the next question:
Building Block Inc. is a multinational company, headquartered in Chicago with offices throughout the United States, Asia, and Europe (including Germany, Italy, France and Portugal). Last year the company was the victim of a phishing attack that resulted in a significant data breach. The executive board, in coordination with the general manager, their Privacy Office and the Information Security team, resolved to adopt additional security measures. These included training awareness programs, a cybersecurity audit, and use of a new software tool called SecurityScan, which scans employees' computers to see if they have software that is no longer being supported by a vendor and therefore not getting security updates. However, this software also provides other features, including the monitoring of employees' computers.
Since these measures would potentially impact employees, Building Block's Privacy Office decided to issue a general notice to all employees indicating that the company will implement a series of initiatives to enhance information security and prevent future data breaches.
After the implementation of these measures, server performance decreased. The general manager instructed the Security team on how to use SecurityScan to monitor employees' computers activity and their location. During these activities, the Information Security team discovered that one employee from Italy was daily connecting to a video library of movies, and another one from Germany worked remotely without authorization. The Security team reported these incidents to the Privacy Office and the general manager. In their report, the team concluded that the employee from Italy was the reason why the server performance decreased.
Due to the seriousness of these infringements, the company decided to apply disciplinary measures to both employees, since the security and privacy policy of the company prohibited employees from installing software on the company's computers, and from working remotely without authorization.
To comply with the GDPR, what should Building Block have done as a first step before implementing the SecurityScan measure?
A. Consulted with the Information Security team to weigh security measures against possible server impacts.
B. Distributed a more comprehensive notice to employees and received their express consent.
C. Assessed potential privacy risks by conducting a data protection impact assessment.
D. Consulted with the relevant data protection authority about potential privacy violations.
Answer: (SHOW ANSWER)

NEW QUESTION: 87
SCENARIO
Please use the following to answer the next question:
Liem, an online retailer known for its environmentally friendly shoes, has recently expanded its presence in Europe. Anxious to achieve market dominance, Liem teamed up with another eco friendly company, EcoMick, which sells accessories like belts and bags. Together the companies drew up a series of marketing campaigns designed to highlight the environmental and economic benefits of their products. After months of planning, Liem and EcoMick entered into a data sharing agreement to use the same marketing database, MarketIQ, to send the campaigns to their respective contacts.

Liem and EcoMick also entered into a data processing agreement with MarketIQ, the terms of which included processing personal data only upon Liem and EcoMick's instructions, and making available to them all information necessary to demonstrate compliance with GDPR obligations.
Liem and EcoMick then procured the services of a company called JaphSoft, a marketing optimization firm that uses machine learning to help companies run successful campaigns. Clients provide JaphSoft with the personal data of individuals they would like to be targeted in each campaign. To ensure protection of its clients' data, JaphSoft implements the technical and organizational measures it deems appropriate. JaphSoft works to continually improve its machine learning models by analyzing the data it receives from its clients to determine the most successful components of a successful campaign. JaphSoft then uses such models in providing services to its client-base. Since the models improve only over a period of time as more information is collected, JaphSoft does not have a deletion process for the data it receives from clients. However, to ensure compliance with data privacy rules, JaphSoft pseudonymizes the personal data by removing identifying information from the contact information. JaphSoft's engineers, however, maintain all contact information in the same database as the identifying information.
Under its agreement with Liem and EcoMick, JaphSoft received access to MarketIQ, which included contact information as well as prior purchase history for such contacts, to create campaigns that would result in the most views of the two companies' websites. A prior Liem customer, Ms. Iman, received a marketing campaign from JaphSoft regarding Liem's as well as EcoMick's latest products. While Ms. Iman recalls checking a box to receive information in the future regarding Liem's products, she has never shopped EcoMick, nor provided her personal data to that company.
For what reason would JaphSoft be considered a controller under the GDPR?
A. It uses personal data to improve its products and services for its client-base through machine learning.
B. It makes decisions regarding the technical and organizational measures necessary to protect the personal data.
C. It has been provided access to personal data in the MarketIQ database.
D. It determines how long to retain the personal data collected.
Answer: (SHOW ANSWER)

NEW QUESTION: 88
Which of the following was the first legally binding international instrument in the area of data protection?
A. EU Directive on Privacy and Electronic Communications.
B. General Data Protection Regulation.
C. Convention 108.
D. Universal Declaration of Human Rights.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 89
SCENARIO
Please use the following to answer the next question:
You have just been hired by a toy manufacturer based in Hong Kong. The company sells a broad range of dolls, action figures and plush toys that can be found internationally in a wide variety of retail stores. Although

the manufacturer has no offices outside Hong Kong and in fact does not employ any staff outside Hong Kong, it has entered into a number of local distribution contracts. The toys produced by the company can be found in all popular toy stores throughout Europe, the United States and Asi a. A large portion of the company's revenue is due to international sales.
The company now wishes to launch a new range of connected toys, ones that can talk and interact with children. The CEO of the company is touting these toys as the next big thing, due to the increased possibilities offered: The figures can answer children's Questions: on various subjects, such as mathematical calculations or the weather. Each figure is equipped with a microphone and speaker and can connect to any smartphone or tablet via Bluetooth. Any mobile device within a 10-meter radius can connect to the toys via Bluetooth as well. The figures can also be associated with other figures (from the same manufacturer) and interact with each other for an enhanced play experience.
When a child asks the toy a QUESTION, the request is sent to the cloud for analysis, and the answer is generated on cloud servers and sent back to the figure. The answer is given through the figure's integrated speakers, making it appear as though that the toy is actually responding to the child's QUESTION. The packaging of the toy does not provide technical details on how this works, nor does it mention that this feature requires an internet connection. The necessary data processing for this has been outsourced to a data center located in South Africa. However, your company has not yet revised its consumer-facing privacy policy to indicate this.
In parallel, the company is planning to introduce a new range of game systems through which consumers can play the characters they acquire in the course of playing the game. The system will come bundled with a portal that includes a Near-Field Communications (NFC) reader. This device will read an RFID tag in the action figure, making the figure come to life onscreen. Each character has its own stock features and abilities, but it is also possible to earn additional ones by accomplishing game goals. The only information stored in the tag relates to the figures' abilities. It is easy to switch characters during the game, and it is possible to bring the figure to locations outside of the home and have the character's abilities remain intact.
In light of the requirements of Article 32 of the GDPR (related to the Security of Processing), which practice should the company institute?
A. Encrypt the data in transit over the wireless Bluetooth connection.
B. Include three-factor authentication before each use by a child in order to ensure the best level of security possible.
C. Insert contractual clauses into the contract between the toy manufacturer and the cloud service provider, since South Africa is outside the European Union.
D. Include dual-factor authentication before each use by a child in order to ensure a minimum amount of security.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 90
SCENARIO
Please use the following to answer the next question:
BHealthy, a company based in Italy, is ready to launch a new line of natural products, with a focus on sunscreen. The last step prior to product launch is for BHealthy to conduct research to decide how

extensively to market its new line of sunscreens across Europe. To do so, BHealthy teamed up with Natural Insight, a company specializing in determining pricing for natural products. BHealthy decided to share its existing customer information - name, location, and prior purchase history - with Natural Insight. Natural Insight intends to use this information to train its algorithm to help determine the price point at which BHealthy can sell its new sunscreens.
Prior to sharing its customer list, BHealthy conducted a review of Natural Insight's security practices and concluded that the company has sufficient security measures to protect the contact information. Additionally, BHealthy's data processing contractual terms with Natural Insight require continued implementation of technical and organization measures. Also indicated in the contract are restrictions on use of the data provided by BHealthy for any purpose beyond provision of the services, which include use of the data for continued improvement of Natural Insight's machine learning algorithms.
In which case would Natural Insight's use of BHealthy's data for improvement of its algorithms be considered data processor activity?
A. If Natural Insight agrees to be fully liable for its use of BHealthy's customer information in its product improvement activities.
B. If Natural Insight uses BHealthy's data for improving price point predictions only for BHealthy.
C. If Natural Insight satisfies the transparency requirement by notifying BHealthy's customers of its plans to use their information for its product improvement activities.
D. If Natural Insight receives express contractual instructions from BHealthy to use its data for improving its algorithms.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 91
What is a reason the European Court of Justice declared the Data Retention Directive invalid in 2014?
A. The requirements affected individuals without exception.
B. The requirements were financially burdensome to EU businesses.
C. The requirements specified that data must be held within the EU.
D. The requirements had limitations on how national authorities could use data.
Answer: D (LEAVE A REPLY)
Reference:
%20the%20Grand,proportionality%20in%20forging%20the%20Directive.

NEW QUESTION: 92

According to the E-Commerce Directive 2000/31/EC, where is the place of "establishment" for a company providing services via an Internet website confirmed by the GDPR?

A. Where the technology supporting the website is located

B. Where the website is accessed

C. Where the decisions about processing are made

D. Where the customer's Internet service provider is located

Answer: D (LEAVE A REPLY)

Explanation/Reference: https://www.ohiobar.org/member-tools-benefits/publications/Ohio-Lawyer/the-european-general- data-protection-regulation-gdpr/

NEW QUESTION: 93

When may browser settings be relied upon for the lawful application of cookies?

A. When users are provided with information about which cookies have been set.

B. When users are aware of the ability to adjust their settings.

C. When a user rejects cookies that are strictly necessary.

D. When it is impossible to bypass the choices made by users in their browser settings.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 94

What is one major goal that the OECD Guidelines, Convention 108 and the Data Protection Directive (Directive
95/46/EC) all had in common but largely failed to achieve in Europe?

A. The establishment of a list of legitimate data processing criteria

B. The creation of legally binding data protection principles

C. The synchronization of approaches to data protection

D. The restriction of cross-border data flow

Answer: D (LEAVE A REPLY)

Explanation/Reference: https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf (99)

NEW QUESTION: 95

Under Article 9 of the GDPR, which of the following categories of data is NOT expressly prohibited from data processing?

A. Personal data revealing financial data.

B. Personal data revealing genetic data.

C. Personal data revealing ethnic origin.

D. Personal data revealing trade union membership.

Answer: (SHOW ANSWER)

NEW QUESTION: 96

When is data sharing agreement MOST likely to be needed?

A. When personal data is being shared between commercial organizations acting as joint data controllers.
B. When personal data is being proactively shared by a controller to support a police investigation.
C. When anonymized data is being shared.
D. When personal data is being shared with a public authority with powers to require the personal data to be disclosed.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 97
Which GDPR principle would a Spanish employer most likely depend upon to annually send the personal data of its employees to the national tax authority?
A. The legitimate interest of the public administration.
B. The legal obligation of the employer.
C. The consent of the employees.
D. The protection of the vital interest of the employees.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 98
SCENARIO
Please use the following to answer the next question:
Anna and Frank both work at Granchester University. Anna is a lawyer responsible for data protection, while Frank is a lecturer in the engineering department. The University maintains a number of types of records:
Student records, including names, student numbers, home addresses, pre-university information, university attendance and performance records, details of special educational needs and financial information.
Staff records, including autobiographical materials (such as curricula, professional contact files, student evaluations and other relevant teaching files).
Alumni records, including birthplaces, years of birth, dates of matriculation and conferrals of degrees. These records are available to former students after registering through Granchester's Alumni portal. Department for Education records, showing how certain demographic groups (such as first-generation students) could be expected, on average, to progress. These records do not contain names or identification numbers.
Under their security policy, the University encrypts all of its personal data records in transit and at rest.
In order to improve his teaching, Frank wants to investigate how his engineering students perform in relational to Department for Education expectations. He has attended one of Anna's data protection training courses and knows that he should use no more personal data than necessary to accomplish his goal. He creates a program that will only export some student data: previous schools attended, grades originally obtained, grades currently obtained and first time university attended. He wants to keep the records at the individual student level. Mindful of Anna's training, Frank runs the student numbers through an algorithm to transform them into different reference numbers. He uses the same algorithm on each occasion so that he can update each record over time.
One of Anna's tasks is to complete the record of processing activities, as required by the GDPR. After receiving her email reminder, as required by the GDPR. After receiving her email reminder, Frank informs Anna about his performance database.

Ann explains to Frank that, as well as minimizing personal data, the University has to check that this new use of existing data is permissible. She also suspects that, under the GDPR, a risk analysis may have to be carried out before the data processing can take place. Anna arranges to discuss this further with Frank after she has done some additional research.
Frank wants to be able to work on his analysis in his spare time, so he transfers it to his home laptop (which is not encrypted). Unfortunately, when Frank takes the laptop into the University he loses it on the train.
Frank has to see Anna that day to discuss compatible processing. He knows that he needs to report security incidents, so he decides to tell Anna about his lost laptop at the same time.
Before Anna determines whether Frank's performance database is permissible, what additional information does she need?
A. More information about Frank's data protection training.
B. More information about what students have been told and how the research will be used.
C. More information about the extent of the information loss.
D. More information about the algorithm Frank used to mask student numbers.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 99
In the event of a data breach, which type of information are data controllers NOT required to provide to either the supervisory authorities or the data subjects?
A. The predicted consequences of the breach.
B. The contact details of the appropriate data protection officer.
C. The measures being taken to address the breach.
D. The type of security safeguards used to protect the data.
Answer: B (LEAVE A REPLY)