

CIPP-E熱門認證-最新考試題庫幫助妳壹次性通過考試



P.S. VCESoft在Google Drive上分享了免費的2026 IAPP CIPP-E考試題庫：https://drive.google.com/open?id=1a__08IBUxEdi21LBkMg8aauRfVksLOU

想要通過CIPP-E認證考試並不是僅僅依靠與考試相關的書籍就可以辦到的。與其盲目地學習考試要求的相關知識，不如做一些有價值的試題。一本高效率的考古題是大家準備考試時必不可少的工具。所以，快點購買VCESoft的CIPP-E考古題吧。這是一本命中率很高的考古題，比其他任何學習方法都有效。这是可以保证你一次就成功的难得的資料。

CIPP/E認證在隱私和數據保護行業中具有很高的聲望，並獲得全球雇主的認可。它是隱私專業人員展示他們在GDPR和歐盟數據保護法和法規方面專業知識的理想認證。該認證還為個人在就業市場上提供了競爭優勢，因為現在許多雇主要求隱私專業人員擁有CIPP/E認證。總的來說，CIPP/E認證對於任何想在歐盟確立自己的隱私專家身份的人來說都是一個有價值的認證。

>> CIPP-E熱門認證 <<

最受推薦的CIPP-E熱門認證，免費下載CIPP-E考試題庫得到妳想要的IAPP證書

VCESoft的專家團隊利用他們的經驗和知識終於研究出了關於IAPP CIPP-E 認證考試的培訓資料。我們的IAPP CIPP-E 認證考試培訓資料很受客戶歡迎，這是VCESoft的專家團隊勤勞勞動的結果。他們研究出來的模擬測試題

及答案有很高的品質，和真實的考試題目有95%的相似性，是很值得你依賴的。如果你使用了VCESoft的培訓工具，你可以100%通過你的第一次參加的IAPP CIPP-E認證考試。

最新的 Certified Information Privacy Professional CIPP-E 免費考試真題 (Q274-Q279):

問題 #274

In which scenario is a Controller most likely required to undertake a Data Protection Impact Assessment?

- A. When personal data is being transferred outside of the EEA.
- **B. When the controller is required to have a Data Protection Officer.**
- C. When personal data is being collected and combined with other personal data to profile the creditworthiness of individuals.
- D. When the controller is collecting email addresses from individuals via an online registration form for marketing purposes.

答案： B

解題說明：

Reference:

%20the%20General, and %20freedoms%20of%20natural%20persons%27.

問題 #275

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 EVERFIT 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 EVERFIT 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 EVERFIT 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 be able to sue any one of the relevant EVERFIT branches, as each one may be held liable for the entire damage.**
- B. He will have to sue the EVERFIT's head office in France, where EVERFIT has its main establishment.
- C. He will have to sue each EVERFIT branch so that each branch provides proportionate compensation commensurate with its contribution to the damage or distress suffered by Javier.
- D. He will be able to apply to the European Data Protection Board in order to determine which particular EVERFIT branch is liable for damages, based on the decision that was made by the board.

答案： A

解題說明：

According to Article 82 of the GDPR¹, any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation from the controller or processor for the damage suffered. Any controller involved in processing shall be liable for the damage caused by processing which infringes the GDPR. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are responsible for

any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject. Therefore, Javier can sue any one of the EVETFIT branches that were involved in processing his personal data without his consent and in violation of his rights, and he can claim full compensation from that branch. The branch that pays the compensation can then claim back from the other branches involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage. Reference: 1 Art. 82 GDPR - Right to compensation and liability - General Data Protection Regulation (GDPR)

問題 #276

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 data. 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.**

答案: D

解題說明:

According to the ePrivacy Directive, which regulates direct electronic marketing in the EU, consent is generally required before sending marketing emails or texts. However, there is an exception known as the 'soft opt-in', which allows marketing emails or texts to be sent on an opt-out basis if the recipient's details were collected "in the context of the sale of a product or a service" and the marketing is for "similar products or services" provided by the same organisation¹². Therefore, WonderKids can send direct marketing information by email without prior consent of the person booking the childcare, as long as the information is about similar products or services to those purchased from WonderKids, and the person is given a clear and easy way to opt out of receiving such emails. The other options are not allowed under the ePrivacy Directive, unless the person has given explicit consent to receive them. Reference:

Free CIPP/E Study Guide, page 33, section 4.1.3

CIPP/E Certification, page 28, section 4.1.3

Cipp-e Study guides, Class notes & Summaries, page 39, section 4.1.3

Direct marketing rules and exceptions under the GDPR, paragraph 5

Marketing | ICO, section "What does the 'soft opt-in' mean?"

問題 #277

Which of the following elements does NOT need to be presented to a data subject in order to collect valid consent for the use of cookies?

- A. Information on the purpose of the cookies.
- **B. A "Cookies Settings" button.**

- C. A list of cookies that may be placed.
- D. A "Reject All" cookies button.

答案： B

解題說明：

According to the EDPB Guidelines 05/2020 on consent under Regulation 2016/6791, valid consent for the use of cookies must meet the following conditions:

*It must be freely given, which means that the data subject must have a genuine choice and the ability to refuse or withdraw consent without detriment.

*It must be specific, which means that the data subject must give consent for each distinct purpose of the processing and for each type of cookie.

*It must be informed, which means that the data subject must receive clear and comprehensive information about the identity of the controller, the purposes of the processing, the types of cookies used, the duration of the cookies, and the possibility of withdrawing consent.

*It must be unambiguous, which means that the data subject must express their consent by a clear affirmative action, such as clicking on an "I agree" button or selecting specific settings in a cookie banner.

*It must be granular, which means that the data subject must be able to consent to different types of cookies separately, such as essential, functional, performance, or marketing cookies.

Therefore, a "Cookies Settings" button is not a necessary element to collect valid consent for the use of cookies, as long as the data subject can exercise their choice and preference through other means, such as a cookie banner with different options. However, a "Cookies Settings" button may be a good practice to enhance transparency and user control, as it allows the data subject to access and modify their consent settings at any time.

On the other hand, a "Reject All" cookies button is a necessary element to collect valid consent for the use of cookies, as it ensures that the data subject can freely refuse consent without detriment. A list of cookies that may be placed and information on the purpose of the cookies are also necessary elements to collect valid consent for the use of cookies, as they ensure that the data subject is informed and can give specific consent for each type of cookie.

References: EDPB Guidelines 05/2020 on consent under Regulation 2016/6791, pages 17-23.

問題 #278

SCENARIO

Please use the following to answer the next question:

Gentle Hedgehog Inc. is a privately owned website design agency incorporated in Italy. The company has numerous remote workers in different EU countries. Recently, the management of Gentle Hedgehog noticed a decrease in productivity of their sales team, especially among remote workers. As a result, the company plans to implement a robust but privacy-friendly remote surveillance system to prevent absenteeism, reward top performers, and ensure the best quality of customer service when sales people are interacting with customers.

Gentle Hedgehog eventually hires Sauron Eye Inc., a Chinese vendor of employee surveillance software whose European headquarters is in Germany. Sauron Eye's software provides powerful remote-monitoring capabilities, including 24/7 access to computer cameras and microphones, screen captures, emails, website history, and keystrokes. Any device can be remotely monitored from a central server that is securely installed at Gentle Hedgehog headquarters. The monitoring is invisible by default; however, a so-called Transparent Mode, which regularly and conspicuously notifies all users about the monitoring and its precise scope, also exists. Additionally, the monitored employees are required to use a built-in verification technology involving facial recognition each time they log in.

All monitoring data, including the facial recognition data, is securely stored in Microsoft Azure cloud servers operated by Sauron Eye, which are physically located in France.

What monitoring may be lawfully performed within the scope of Gentle Hedgehog's business?

- A. Only emails, website browsing history and camera for internal video calls that are expressly marked as monitored.
- B. Everything offered by Sauron Eye's software, assuming employees provide daily consent to the monitoring.
- C. Only video calls conducted during business hours and emails that do not contain a "private" or "personal" tag.
- D. Everything offered by Sauron Eye's software with the exception of camera and microphone monitoring.

答案： A

解題說明：

The General Data Protection Regulation (GDPR) does not prohibit surveillance of employees in the workplace. Still, it requires employers to follow special rules to ensure that the rights and freedoms of employees are protected when processing their personal data. The GDPR applies to any processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not. The GDPR also applies to the processing of

personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to the offering of goods or services to data subjects in the EU or the monitoring of their behaviour as far as their behaviour takes place within the EU.

The GDPR requires that any processing of personal data must be lawful, fair and transparent, and based on one of the six legal grounds specified in the regulation. The most relevant legal grounds for employee surveillance are the legitimate interests of the employer, the performance of a contract with the employee, or the compliance with a legal obligation. The GDPR also requires that any processing of personal data must be limited to what is necessary for the purposes for which they are processed, and that the data subjects must be informed of the purposes and the legal basis of the processing, as well as their rights and the safeguards in place to protect their data.

The GDPR also imposes specific obligations and restrictions on the processing of special categories of personal data, such as biometric data, which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or which are processed for the purpose of uniquely identifying a natural person. The processing of such data is prohibited, unless one of the ten exceptions listed in the regulation applies. The most relevant exceptions for employee surveillance are the explicit consent of the data subject, the necessity for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, or the necessity for reasons of substantial public interest.

The GDPR also sets out the rules and requirements for the transfer of personal data to third countries or international organisations, which do not ensure an adequate level of data protection. The transfer of such data is only allowed if the controller or processor has provided appropriate safeguards, such as binding corporate rules, standard contractual clauses, codes of conduct or certification mechanisms, and if the data subjects have enforceable rights and effective legal remedies.

Based on the scenario, the only monitoring that may be lawfully performed within the scope of Gentle Hedgehog's business is the monitoring of emails, website browsing history and camera for internal video calls that are expressly marked as monitored. This option is the most consistent with the GDPR's principles and requirements, as it:

Is based on the legitimate interests of the employer to ensure the productivity, quality and security of the work performed by the employees, as well as the performance of a contract with the employees and the compliance with a legal obligation to prevent fraud and protect confidential information.

Is limited to what is necessary for the purposes of the monitoring, as it only covers the work-related activities and communications of the employees, and excludes the private or personal ones.

Is transparent to the employees, as it informs them of the monitoring and its precise scope, and gives them the opportunity to object or opt out of the monitoring.

Does not involve the processing of special categories of personal data, such as biometric data or data revealing political opinions or trade union membership, which are not necessary or proportionate for the purposes of the monitoring.

Does not involve the transfer of personal data to a third country, such as China, which does not provide an adequate level of data protection, and which may pose additional risks for the rights and freedoms of the employees.

The other options listed in the question are not lawful monitoring within the scope of Gentle Hedgehog's business, as they:

Are not based on a valid legal ground for the processing of personal data, as they either rely on the consent of the employees, which is not freely given, informed and specific, or on the legitimate interests of the employer, which are not balanced with the rights and freedoms of the employees.

Are not limited to what is necessary for the purposes of the monitoring, as they involve the collection and processing of excessive and irrelevant personal data, such as camera and microphone monitoring, screen captures, keystrokes, and facial recognition data, which go beyond the scope of the work performed by the employees, and intrude into their private or personal sphere.

Are not transparent to the employees, as they do not inform them of the monitoring and its precise scope, and do not give them the opportunity to object or opt out of the monitoring.

Involve the processing of special categories of personal data, such as biometric data or data revealing political opinions or trade union membership, which are not necessary or proportionate for the purposes of the monitoring, and which do not fall under any of the exceptions listed in the regulation.

Involve the transfer of personal data to a third country, such as China, which does not provide an adequate level of data protection, and which may pose additional risks for the rights and freedoms of the employees.

Reference:

GDPR, Articles 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 44, 45, 46, 47, 48, and 49.

EDPB Guidelines 3/2019 on processing of personal data through video devices, pages 5, 6, 7, 8, 9, 10, 11, 12, 13, and 14.

EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, pages 19, 20, 21, 22, 23, 24, 25, 26, 27, and 28.

EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, pages 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, and 28.

EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, pages 4, 5, 6, 7, 8, 9, 10, 11, and 12.

Data protection: GDPR and employee surveillance | Feature | Law Gazette, paragraphs 1, 2, 3, 4, 5, 6, 7, and 8.

VCESoft的產品是為你們參加IAPP CIPP-E認證考試而準備的。VCESoft提供的培訓資料不僅包括與IAPP CIPP-E認證考試相關的資訊技術培訓資料，來鞏固專業知識，而且還有準確性很高的關於IAPP CIPP-E的認證考試的相關考試練習題和答案。可以保證你第一次參加IAPP CIPP-E的認證考試就以高分順利通過。

我們最終學習和掌握了多少專業知識和技能 and CIPP-E 考試並沒有非常直接的關係，在練習 CIPP-E 問題集的同時做好總結，VCESoft CIPP-E 題庫能為參加 IT 相關認證考試的考生提供他們想要的資料來助幫助他們通過考試，你可以先從通過 CIPP-E 認證考試開始，因為這是 IAPP 的一個非常重要的考試，值得信賴的 CIPP-E 題庫 - Certified Information Privacy Professional/Europe (CIPP/E) 考古題，不通過，全額退款，VCESoft CIPP-E 題庫就能為你提高品質有效的考古題，提供 IAPP CIPP-E 題庫認證學習、考試資料、免費的 IBM 官方原版培訓、自學教程-IT 認證題庫網，IAPP CIPP-E 熱門認證 在現在這個人才濟濟的社會裏，還是有很多行業是缺乏人才的，比如 IT 行業就相當缺乏技術性的人才。

桑子明跟著師傅黃瑞，來到仙文館門口，啊！林夕麒忽然驚呼了壹聲，我們最終學習和掌握了多少專業知識和技能，和CIPP-E考試並沒有非常直接的關係，在練習CIPP-E問題集的同時做好總結，VCESoft能為參加IT相關認證考試的考生提供他們想要的資料來助幫助他們通過考試。

你可以先從通過CIPP-E認證考試開始，因為這是IAPP的一個非常重要的考試，值得信賴的 Certified Information Privacy Professional/Europe (CIPP/E) 考古題，不通過，全額退款。

- 順便提一下，可以從雲存儲中下載VCESoft CIPP-E考試題庫的完整版：https://drive.google.com/open?id=1a_08IBUxEdi21LBkMg8aauRfVksLOU

順便提一下，可以從雲存儲中下載VCESoft CIPP-E考試題庫的完整版：https://drive.google.com/open?id=1a_08IBUxEdi21LBkMg8aauRfVksLOU