PassQueen
a.k.a dumpsqueen.com

Certified Information Privacy Professional/Europe (CIPP/E)

IAPP CIPP-E

Version Demo

Total Demo Questions: 40

Total Premium Questions: 400

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Introduction to European Data Protection	22
Topic 2, European Data Protection Law and Regulation	224
Topic 3, Compliance with European Data Protection Law and Regulation	154
Total	400

QUESTION NO: 1

SCENARIO

Please use the following to answer the next question:

Zandelay Fashion (â€˜Zandelayâ€™) 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 companyâ€™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 companyâ€™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 Zandelayâ€™s business plan and associated processing activities.

What would MOST effectively assist Zandelay in conducting their data protection impact assessment?

A. Information about DPIAs found in Articles 38 through 40 of the GDPR.

B. Data breach documentation that data controllers are required to maintain.

C. Existing DPIA guides published by local supervisory authorities.

D. Records of processing activities that data controllers are required to maintain.

ANSWER: C

Explanation:

Existing DPIA guides published by local supervisory authorities would most effectively assist Zandelay because they translate the GDPR's general DPIA obligations into a practical process that the organisation can apply to its proposed app and loyalty scheme. This processing includes systematic profiling of customers' purchase behaviour, potentially affects children, and uses financial information, making a structured assessment of likely risks to individuals particularly important. Under Article 35, a DPIA must describe the envisaged processing and purposes, assess necessity and proportionality, identify risks to data subjects' rights and freedoms, and document measures intended to address those risks. Supervisory-authority guidance commonly supplies usable screening questions, assessment templates, risk methodologies, and examples of safeguards. These resources help the DPO obtain the necessary information from product, marketing, security, and business teams, demonstrate accountability, and produce a DPIA that supports a well-founded decision on whether residual high risk requires prior consultation. The Irish Data Protection Commissioner's DPIA guidance is especially pertinent because Zandelay is established in Ireland and the Irish authority would be the relevant lead supervisory authority for this processing. The underlying legal requirements are set out in GDPR Article 35; practical Irish guidance is available from the Data Protection Commission.

QUESTION NO: 2

If a French controller has a car-sharing app available only in Morocco, Algeria and Tunisia, but the data processing activities are carried out by the appointed processor in Spain, the GDPR will apply to the processing of the personal data so long as?

A. The individuals are European citizens or residents.

B. The data processing activities are in Spain.

C. The data controller is in France.

D. The EU individuals are targeted.

ANSWER: C

Explanation:

The data controller is in France. The GDPR applies under Article 3(1) because the controller is established in France, an EU Member State, and the processing is carried out in the context of that establishment's activities. Article 3(1) is not limited by the nationality, residence, or physical location of the people whose data is processed. Nor does it depend on whether the app is offered only in non-EU countries. The decisive connection is the controller's EU establishment and the relationship between that establishment's activities and the processing operation. In this scenario, the French controller determines the purposes and means of the car-sharing app's personal-data processing and appoints a processor to perform processing activities. Using a processor in Spain does not displace the controller's GDPR responsibilities; rather, the processing remains subject to the GDPR where it is undertaken in the context of the French controller's establishment. Article 3(1) expressly provides that this result applies regardless of whether the processing itself takes place in the Union. See GDPR, Article 3 and the EDPB Guidelines on the territorial scope of the GDPR.

QUESTION NO: 3

Which kind of privacy notice, originally advocated by the Article 29 Working Party, is commonly recommended tor AI-based technologies because of the way it provides processing information at specific points of data collection?

A. Privacy dashboard notice

B. Visualization notice.

C. Just-in-time notice.

D. Layered notice.

ANSWER: C

Explanation:

Just-in-time notice is correct because it delivers relevant transparency information at the moment a person is about to provide personal data or use a feature that triggers a particular processing activity. Rather than requiring individuals to locate and interpret all relevant details in a long general privacy policy, this approach presents the information in the context in which it is needed. For example, an AI-enabled application can show a short notice when a user activates voice input, uploads an image, enables location-based functionality, or submits information that will be used to train or improve a model.

This contextual timing is particularly useful for AI-based technologies, whose data uses and consequences may not be obvious from the interface alone. It supports the GDPR transparency principle by making information concise, intelligible, easily accessible, and provided at an appropriate time. The Article 29 Working Party's transparency guidance expressly identifies just-in-time notices as a useful method for providing information in a specific context, including when personal data are collected. Such notices can operate alongside a full privacy notice, giving users immediate essential information while preserving access to more detailed material. See the Article 29 Working Party Guidelines on Transparency and the ICO's guidance on explaining AI decisions.

QUESTION NO: 4

To which of the following parties does the territorial scope of the GDPR NOT apply?

A. All member countries of the European Economic Area.

B. All member countries party to the Treaty of Lisbon.

C. All member countries party to the Paris Agreement.

D. All member countries of the European Union.

ANSWER: C

Explanation:

All member countries party to the Paris Agreement is correct because the Paris Agreement is an international climate treaty with parties around the world; membership does not create any connection to the EU data-protection legal framework. The GDPR's territorial scope is instead determined by Article 3. It applies to processing in the context of an establishment in the Union, regardless of where processing occurs. It can also apply to controllers or processors outside the Union when they offer goods or services to people in the Union or monitor those people's behaviour there. The GDPR is directly applicable in all EU Member States. In addition, through the EEA Agreement and related incorporation mechanisms, substantively equivalent GDPR rules apply throughout the European Economic Area, including the relevant EFTA states. The Treaty of Lisbon is an EU treaty, so its Member State parties are within the EU legal order to which the GDPR applies. By contrast, being a Paris Agreement party alone says nothing about whether an organisation is established in the Union, targets individuals there, or monitors their behaviour. See the GDPR's territorial-scope rule in Article 3 of Regulation (EU) 2016/679 and the UNFCCC overview of the Paris Agreement.

QUESTION NO: 5

According to the European Data Protection Board, controllers responding to a data subject access request can refuse to provide a copy of personal data under certain conditions. Which of the following is NOT one of these conditions?

A. If the data subject access request was sent to an employee that is not involved in the processing of such requests.

B. If there is such a large amount of data that the controller cannot identify the data subject of the request.

C. If the controller is unable to use end-to-end encrypted emails for responding to such requests.

D. If the personal data was processed in the past but is no longer at the controller's disposal at the time of the request.

ANSWER: C

Explanation:

If the controller is unable to use end-to-end encrypted emails for responding to such requests, that inability is not a ground to refuse a data subject's request for a copy of their personal data. Article 15(3) GDPR requires the controller to provide a copy of the personal data undergoing processing, while Article 12(1) requires communications and actions relating to data-subject rights to be facilitated. The GDPR does not prescribe end-to-end encrypted email as the only permissible delivery channel. Instead, the controller must select an appropriate means of communicating the copy and apply security measures proportionate to the risk, consistent with the integrity and confidentiality principle in Article 5(1)(f) and the security-of-processing obligations in Article 32. Depending on the circumstances, this may include a secure portal, encrypted attachment with the password sent separately, verified collection, or postal delivery. The EDPB's access-right guidance likewise stresses that controllers must facilitate exercise of the right and provide the copy in a secure manner; the particular transmission technology is not itself a condition limiting the right. See GDPR, especially Articles 12, 15 and 32 and the EDPB Guidelines 01/2022 on the right of access.

QUESTION NO: 6

A company is hesitating between Binding Corporate Rules and Standard Contractual Clauses as a global data transfer solution. Which of the following statements would help the company make an effective decision?

A. Binding Corporate Rules are especially recommended for small and medium companies.

B. The data exporter does not need to be located in the EU for the standard Contractual Clauses.

C. Binding Corporate Rules provide a global solution for all the entities of a company that are bound by the intra-group agreement.

D. The company will need the prior authorization of all EU data protection authorities for concluding Standard Contractual Clauses.

ANSWER: C

Explanation:

Binding Corporate Rules provide a global solution for all the entities of a company that are bound by the intra-group agreement. BCRs are designed specifically for multinational groups of undertakings, or groups of enterprises engaged in a joint economic activity, that make recurring personal-data transfers among their own members across jurisdictions. Once approved by the competent supervisory authority through the GDPR cooperation process, the rules create a consistent, organisation-wide framework for transfers from group entities subject to the GDPR to group entities in third countries. They must be legally binding on the participating entities and enforceable by data subjects, and must include the safeguards and commitments specified by Article 47, such as a complaint process, liability arrangements, training, auditing, and cooperation with supervisory authorities. This makes BCRs particularly useful where a company needs an enduring, scalable transfer mechanism across many affiliates rather than separate contractual arrangements for each transfer relationship. The European Commission identifies BCRs as an appropriate safeguard for transfers within a corporate group, while the EDPB explains their role as a framework for global intra-group data flows. See GDPR Article 47 and the EDPB guide on international data transfers.

QUESTION NO: 7

Since blockchain transactions are classified as pseudonymous, are they considered to be within the material scope of the GDPR, or outside of it?

A. Outside the material scope of the GDPR, because transactions do not include personal data about data subjects in the European Union.

B. Outside the material scope of the GDPR, because transactions are for personal or household purposes.

C. Within the material scope of the GDPR where transactions relate to identifiable natural persons, because pseudonymised data remains personal data.

D. Within the material scope of the GDPR but outside of the territorial scope, because blockchains are decentralized.

ANSWER: C

Explanation:

Within the material scope of the GDPR where transactions relate to identifiable natural persons, because pseudonymised data remains personal data. Article 2(1) GDPR covers processing of personal data that is wholly or partly automated; blockchain validation, recording, and transaction processing are automated operations. Article 4(1) defines personal data broadly as information relating to an identified or identifiable natural person, including identification through an online identifier or other indirect means. A blockchain address, public key, transaction history, or associated metadata may permit a person to be singled out or linked to identity information held elsewhere. Pseudonymisation reduces the direct link between data and an individual, but does not remove the possibility of identification. Recital 26 specifically confirms that pseudonymised personal data that could be attributed to a natural person through additional information remains information on an identifiable natural person. Thus, categorising transactions as pseudonymous does not place them outside the GDPR's material scope. Whether the GDPR applies in a particular cross-border situation also requires a separate assessment of its territorial scope under Article 3; that issue does not alter the material-scope conclusion. See GDPR, Articles 2 and 4 and GDPR, Recital 26.

QUESTION NO: 8

Which statement provides an accurate description of a directive?

A. A directive specifies certain results that must be achieved, but each member state is free to decide how to turn it into a national law.

B. A directive has binding legal force throughout every member state and enters into force on a set date in all the member states.

C. A directive is a legal act relating to specific cases and directed towards member states, companies 0' private individuals.

D. A directive is a legal act that applies automatically and uniformly to all EU countries as soon as it enters into force.

ANSWER: A

Explanation:

A directive specifies the result that must be achieved while allowing each Member State discretion over the form and methods used to implement it in national law. This reflects Article 288 of the Treaty on the Functioning of the European Union: a directive is binding, as to the result to be achieved, upon every Member State to which it is addressed, while national authorities retain competence regarding the choice of implementation measures. Directives therefore commonly require transposition through domestic legislation, regulations, or other national legal measures by a stated deadline. This structure permits EU law to establish a common policy outcome while accommodating differences among national legal systems and administrative arrangements. For privacy professionals, this distinction is important when assessing the source and practical application of European data-protection obligations: a directive's requirements are generally given effect through the relevant national implementing law. The EU's official legal glossary likewise describes directives as acts setting goals for EU countries while leaving them free to choose how those goals are achieved. See Article 288 TFEU on EUR-Lex and the EUR-Lex definition of a directive.

QUESTION NO: 9

According to the GDPR. Article 4(14). biometric data is defined as:

"Personal data resulting from specific technical processing relating to the_____charactenstics of a natural person"

Which term could NOT be placed in the above definition?

A. Psychological.

B. Physical.

C. Intellectual.

D. Behavioral

E. Both Psychological and Intellectual.

ANSWER: E

Explanation:

Both "Psychological" and "Intellectual" could not be placed in the quoted portion of the definition. Article 4(14) GDPR defines biometric data as personal data resulting from specific technical processing relating to the *physical, physiological or behavioural* characteristics of a natural person, where that processing allows or confirms unique identification. The statutory wording is deliberately specific: it identifies the types of characteristics from which biometric data may result and links them to technical processing used for identification. Therefore, because the question is framed as single choice but contains two terms that do not appear in the legal definition, the accurate answer must identify both of them together. This preserves the GDPR's exact terminology rather than treating "physical" as excluded; physical characteristics are expressly included. The complete definition is available in Article 4(14) of the GDPR text on EUR-Lex. For additional regulatory context, the European Data Protection Board discusses biometric data as a special-category-data context in its SME data protection guide.

QUESTION NO: 10

A data controller appoints a data protection officer. Which of the following conditions would NOT result in an infringement of Articles 37 to 39 of the GDPR?

A. If the data protection officer lacks ISO 27001 auditor certification.

B. If the data protection officer is provided by the data processor.

C. If the data protection officer also manages the marketing budget.

D. If the data protection officer receives instructions from the data controller.

ANSWER: A

Explanation:

"If the data protection officer lacks ISO 27001 auditor certification." would not, by itself, infringe Articles 37 to 39 of the GDPR. Article 37 requires that a data protection officer be designated on the basis of professional qualities and, in particular, expert knowledge of data-protection law and practices. The necessary level of expertise must be assessed in light of the processing operations performed and the protection required for the personal data processed. The GDPR does not prescribe any particular professional credential, ISO qualification, or auditor certification as a condition of serving as a data protection officer. ISO/IEC 27001 concerns information-security management systems and an auditor credential may be useful evidence of relevant experience in some contexts, but it is not a statutory requirement for appointment. The controller must instead ensure that the appointed officer can carry out the role's GDPR tasks, including informing and advising the organization, monitoring compliance, providing advice on data-protection impact assessments, and cooperating with the supervisory authority. The designation can therefore remain compliant despite the absence of this specific certification, provided the officer has appropriate expertise and is properly supported in performing the role. See GDPR Articles 37–39 on EUR-Lex and the EDPB guidance on data protection officers.

QUESTION NO: 11

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.

In addition to notifying employees about the purpose of the monitoring, the potential uses of their data and their privacy rights, what information should Building Block have provided them before implementing the security measures?

A. Information about what is specified in the employment contract.

B. Information about who employees should contact with any queries.

C. Information about how providing consent could affect them as employees.

D. Information about how the measures are in the best interests of the company.

ANSWER: B

Explanation:

Information about who employees should contact with any queries is required as part of transparent processing information. Before SecurityScan is used to process employee activity and location data, Building Block must provide the identity and

contact details of the controller and, where applicable, the contact details of its data protection officer. This gives employees a practical, accessible route to ask questions about the monitoring, exercise data-subject rights, or raise concerns about the processing. A general announcement that security initiatives will occur is not enough when the tool processes identifiable employee data for monitoring and possible disciplinary purposes.

Under GDPR Article 13, where personal data are collected directly from employees, the controller must provide specified information at the time of collection, including controller contact details and DPO contact details where applicable. This transparency obligation supports the fairness principle in Article 5(1)(a), particularly in the employment context, where the employer has greater power and workers need clear information about how to engage with the organization regarding monitoring. The information should be communicated in a concise, transparent, intelligible and easily accessible form. See GDPR, especially Articles 5, 12 and 13 and the EDPB guide on respecting individuals' rights.

QUESTION NO: 12

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.

Which statement accurately summarizes Bedrock's obligation in regard to Louis's data portability request?

A. Bedrock does not have a duty to transfer Louis's data to Zantrum if doing so is legitimately not technically feasible.

B. Bedrock does not have to transfer Louis's data to Zantrum because the right to data portability does not apply where personal data are processed in order to carry out tasks in the public interest.

C. Bedrock has failed to comply with the duty to transfer Louis's data to Zantrum because the duty applies wherever personal data are processed by automated means and necessary for the performance of a contract with the customer.

D. Bedrock has failed to comply with the duty to transfer Louis's data to Zantrum 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: A

Explanation:

Bedrock does not have a duty to transfer Louis's data to Zantrum if doing so is legitimately not technically feasible. Article 20(2) GDPR gives a data subject the right to have personal data transmitted directly from one controller to another, but expressly qualifies that right: direct transmission is required only "where technically feasible." Thus, although Louis may exercise portability for data he provided that are processed by automated means under the relevant lawful basis, Bedrock's direct controller-to-controller transmission obligation is limited by the practical technical-feasibility condition. Bedrock has provided Louis with an XML version of his No Claims Certificate, which is a structured, machine-readable format and can enable Louis to provide relevant information to Zantrum himself. The fact pattern specifically states that direct transmission is not technically feasible; on that stated premise, Bedrock is not obliged by Article 20(2) to send the data directly to Zantrum. The GDPR does not impose an absolute requirement that every controller create a direct-transfer connection with every other insurer. Article 20 also clarifies that exercising portability must not adversely affect the rights and freedoms of others. See GDPR, Article 20 and the EDPB's Guidelines on the right to data portability.

QUESTION NO: 13

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 data. 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.

Emily sends the draft to Sam for review. Which of the following is Sam most likely to point out as the biggest problem with Emily's consent provision?

A. It is not legal to include fields requiring information regarding health status without consent.

B. Processing health data requires explicit consent, but the form does not ask for explicit consent.

C. Direct marketing requires explicit consent, whereas the registration form only provides for a right to object

D. The provision of the fitness app should be made conditional on the consent to the data processing for direct marketing.

ANSWER: B

Explanation:

Processing health data requires explicit consent, but the form does not ask for explicit consent. The GDPR treats data concerning health as a special category of personal data. This includes information about a person's physical or mental health, including information collected while providing health-related services that reveals their health status. An app that records diet, exercise, sleep patterns, health status, and related data will commonly process such protected information.

Under Article 9, processing special-category data is prohibited unless a specified exception applies. In this scenario, the relevant exception is the data subject's *explicit* consent. Vigotron's general statement that the user consents to processing "personal data" for use of the app does not clearly and expressly identify health data or obtain explicit consent for that special-category processing. Consent must also be specific, informed, and demonstrated through a clear affirmative act. The registration and consent design should therefore separately and clearly request explicit agreement to the processing of health data for the defined functions of M-Health, while providing the required information about the processing.

Article 9(1)–(2)(a) establishes the special protection and explicit-consent condition for health data: GDPR, Article 9. The GDPR's definition of data concerning health is in Article 4(15).

QUESTION NO: 14

Please select **4 of the 7 options below** . No partial credit will be given.

Which of the following are considered core data protection principles under the GDPR?

A. Purpose limitation.

B. Individual participation.

C. Data minimization.

D. Access and correction.

E. Storage limitation.

F. Data localization.

G. Integrity and confidentiality.

ANSWER: A C E G

Explanation:

"Purpose limitation," "Data minimization," "Storage limitation," and "Integrity and confidentiality" are core GDPR data-processing principles because each is expressly set out in Article 5(1) of the GDPR. Purpose limitation requires that personal data be collected for specified, explicit and legitimate purposes, with subsequent processing remaining compatible with those stated purposes. Data minimization requires controllers to ensure that data are adequate, relevant and limited to what is necessary for the processing purpose. Storage limitation requires personal data to be retained in identifiable form for no longer than necessary, subject to the GDPR's provisions for certain archiving, research and statistical purposes. Integrity and confidentiality, often called the security principle, requires appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

These principles operate throughout the data lifecycle, from deciding what data to collect through defining retention practices and implementing security safeguards. They also support the accountability obligation in Article 5(2), under which the controller must be able to demonstrate compliance with the Article 5(1) principles. The authoritative text is available in Regulation (EU) 2016/679, Article 5; see also the European Commission's overview of EU data-protection rules.

QUESTION NO: 15

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. Getting consent from the data subject for a cross border data transfer.

D. Encrypting data in transit and at rest using strong encryption algorithms.

ANSWER: B

Explanation:

Conducting regular audits of the data protection program demonstrates the GDPR accountability principle because accountability requires a controller not only to comply with the data-protection principles in Article 5(1), but also to be able to demonstrate that compliance. Recurring audits provide documented, reviewable evidence that the organization evaluates whether its policies, operational controls, processing activities, vendor arrangements, security measures, and staff practices remain aligned with GDPR obligations. They also support identification and remediation of gaps, helping ensure that compliance is maintained over time rather than treated as a one-time exercise.

Article 5(2) expressly places this responsibility on the controller. This is reinforced by Article 24, which requires controllers to implement appropriate technical and organisational measures and to review and update them where necessary. Audit records, findings, remediation plans, and follow-up reviews can therefore form part of the demonstrable evidence expected under an accountable privacy-management program. The European Data Protection Board similarly emphasizes that accountability entails putting appropriate measures in place and being able to show their effectiveness. See GDPR, Articles 5 and 24 and the EDPB data protection guide.

QUESTION NO: 16

Which institution has the power to adopt findings that confirm the adequacy of the data protection level in a non-EU country?

A. The European Parliament

B. The European Commission

C. The Article 29 Working Party

D. The European Council

ANSWER: B

Explanation:

The European Commission has the power to adopt an adequacy decision finding that a non-EU country, territory, specified sector, or international organisation ensures an adequate level of protection for personal data. This authority is established by Article 45 of the GDPR. Before adopting a decision, the Commission assesses matters such as the rule of law, respect for human rights and fundamental freedoms, relevant data-protection legislation, effective and enforceable data-subject rights, and the existence and functioning of an independent supervisory authority. The Commission must also obtain an opinion from the European Data Protection Board and follow the applicable comitology procedure. An adequacy decision enables personal data to flow from the European Economic Area to the covered destination without exporters needing to put in place additional transfer safeguards, such as standard contractual clauses, for transfers within the scope of that decision. Adequacy decisions are subject to periodic review, at least every four years, and the Commission may amend, suspend, or repeal a decision if the level of protection is no longer adequate. See GDPR Article 45 in Regulation (EU) 2016/679 and the European Commission's adequacy decisions guidance.

QUESTION NO: 17

Which of the following is NOT a role of works councils?

A. Determining the monetary fines to be levied against employers for data breach violations of employee data.

B. Determining whether to approve or reject certain decisions of the employer that affect employees.

C. Determining whether employees' personal data can be processed or not.

D. Determining what changes will affect employee working conditions.

ANSWER: A

Explanation:

Determining the monetary fines to be levied against employers for data breach violations of employee data is not a role of a works council. Works councils are employee-representation bodies established under national labour law. Their functions commonly include information, consultation and, for specified workplace matters, co-determination with the employer. In the employment-privacy context, this can include involvement in policies or technical arrangements that affect employees, such as systems used to monitor staff or process workforce information. Their role is therefore rooted in collective labour relations rather than public-law enforcement.

Administrative fines for infringements of data-protection law are imposed by the competent supervisory authority, not by an employer or its works council. Article 83 of the GDPR requires each supervisory authority to ensure that administrative fines are imposed in an effective, proportionate and dissuasive manner, subject to procedural safeguards under EU and Member State law. The GDPR also assigns supervisory authorities investigation and corrective powers, including the power to impose administrative fines. This division preserves the independence of regulatory enforcement while allowing works councils to protect employees' workplace interests through their representative and co-determination functions. See Regulation (EU) 2016/679 (GDPR), especially Articles 58 and 83 and the European Commission's data-protection overview.

QUESTION NO: 18

Bioface is a company based in the United States. It has no servers, personnel or assets in the European Union. By collecting photographs from social media and other web-based services, such as newspapers and blogs, it uses machine learning to develop a facial recognition algorithm. The algorithm identifies individuals in photographs who are not in its data set based the algorithm and its existing data. The service collects photographs of data subjects in the European Union and will identify

them if presented with their photographs. Bioface offers its service to government agencies and companies in the United States and Canada, but not to those in the European Union. Bioface does not offer the service to individuals.

Why is Bioface subject to the territorial scope of the General Data Protection Regulation?

A. It collects data from European Union websites, which constitutes an establishment in the European Union.

B. It offers services in the European Union by identifying data subjects in the European Union.

C. It collects data from subjects and uses it for automated processing.

D. It monitors the behavior of data subjects in the European Union.

ANSWER: D

Explanation:

It monitors the behavior of data subjects in the European Union. Article 3(2)(b) GDPR applies to a controller or processor that is not established in the European Union where its processing relates to monitoring the behaviour of people in the Union, insofar as that behaviour takes place there. Bioface's lack of EU staff, assets, servers, or customers therefore does not prevent the GDPR from applying. Its facial-recognition service processes images of people in the Union to recognise and identify them through an algorithm and an existing image dataset. This is a form of observation and assessment of identifiable individuals that falls within the GDPR's monitoring limb when undertaken in relation to people in the EU. The territorial rule is designed to ensure that an overseas organisation cannot avoid GDPR obligations merely by operating from outside the Union while using technology to observe individuals within it. The European Data Protection Board specifically identifies monitoring activities as a basis for Article 3(2) applicability and explains that the assessment depends on the processing activity and its connection to behaviour in the Union. See GDPR, Article 3 and the EDPB Guidelines on the territorial scope of the GDPR.

QUESTION NO: 19

Under what circumstances would the GDPR apply to personal data that exists in physical form, such as information contained in notebooks or hard copy files?

A. Only where the personal data is produced as a physical output of specific automated processing activities, such as printing, labelling, or stamping.

B. Only where the personal data is to be subjected to specific computerized processing, such as imagescanning or optical character recognition.

C. Only where the personal data is treated by automated means in some way, such as computerized distribution or filing.

D. Only where the personal data is handled in a sufficiently structured manner so as to form part of a filing system.

ANSWER: D

Explanation:

Only where the personal data is handled in a sufficiently structured manner so as to form part of a filing system is correct because the GDPR expressly extends its material scope to non-automated processing of personal data when that data forms part of a filing system, or is intended to form part of one. This ensures that structured paper records cannot fall outside data-protection obligations merely because they are not stored electronically. A filing system is any structured set of personal data that is accessible according to specific criteria; it need not be centrally organised or indexed in a sophisticated way. For example, personnel records arranged by employee name, customer files organised by account number, or paper case files retrievable by a defined identifier can constitute a filing system. The key point is that the records are structured so that information relating to particular individuals can be accessed using specified criteria. Article 2(1) sets out this scope, while Recital 15 clarifies that the Regulation covers manual filing systems where they are structured according to specific criteria. Accordingly, physical format alone does not remove data from the GDPR's scope when the paper records are part of such an organised system. See GDPR, Article 2(1) and GDPR, Recital 15.

QUESTION NO: 20

Which sentence BEST summarizes the concepts of “fairness,” “lawfulness” and “transparency”, as expressly required by Article 5 of the GDPR?

A. Fairness means processing personal data in ways individuals would reasonably expect and not using it in unjustifiably detrimental, discriminatory, deceptive, or misleading ways; lawfulness requires a valid GDPR legal basis; transparency requires clear, accessible information about the processing.

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

Explanation:

“Fairness means processing personal data in ways individuals would reasonably expect and not using it in unjustifiably detrimental, discriminatory, deceptive, or misleading ways; lawfulness requires a valid GDPR legal basis; transparency requires clear, accessible information about the processing” best captures the three distinct, cumulative requirements in Article 5(1)(a) GDPR. Lawfulness means that each processing activity must be grounded in one of the legal bases set out in Article 6, such as consent, performance of a contract, compliance with a legal obligation, protection of vital interests, a public task, or legitimate interests where applicable. Fairness is broader than merely giving notice: it concerns the substance and effect of processing on the individual, including whether the processing is reasonable in context. Transparency requires controllers to communicate information about processing openly and intelligibly, using concise, clear, and plain language, so that people can understand how and why their data are used. These principles apply throughout the processing lifecycle, rather than being limited to the point of collection. Article 5 establishes the governing principles, while Articles 12 through 14 operationalize transparency through information duties. See GDPR, Articles 5, 6 and 12–14 and the EDPB Guidelines on Transparency.

QUESTION NO: 21

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 essentially functions as a one-stop shop mechanism

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 makes appointment of a data protection officer mandatory

ANSWER: B

Explanation:

That it takes the form of a Regulation as opposed to a Directive is correct because a Regulation is directly applicable in every Member State. It does not normally need to be transposed into separate national legislation before it takes effect. This legal form therefore establishes a common baseline of rules, rights, obligations, and enforcement requirements across the European Union from the same instrument and effective date. By contrast, directives set objectives that Member States must implement through their own domestic laws, which can result in differences in wording, timing, and national implementation choices. The GDPR was deliberately adopted as a Regulation to strengthen harmonisation of data-protection law and facilitate more consistent protection for individuals and more predictable compliance expectations for organisations operating across borders. Although the GDPR permits limited national specifications in particular areas, its directly applicable nature remains the principal structural feature supporting consistency throughout the Union. The European Commission describes the GDPR as a regulation that provides rules directly applicable across Member States, while Article 288 of the Treaty on the

Functioning of the European Union explains that regulations are binding in their entirety and directly applicable. See the European Commission’s data-protection overview and Article 288 TFEU.