When you want to log into your account, sometimes you need both your password and an extra code sent to your phone. This is called two-factor authentication. What is it?

a) A type of privacy app

b) A method to secure your online accounts by requiring two different forms of identification

c) A popular online video streaming service

d) A social networking site

b) A method to secure your online accounts by requiring two different forms of identification.

What do people mean by 'Virtual Private Network' (VPN) when talking about online privacy?

a) A platform for online gaming

b) A social media network

c) A tool to encrypt and protect your internet connection and data

d) A virtual reality headset

c) A tool to encrypt and protect your internet connection and data.

In terms of privacy, what does the term "metadata" mean?

a) A type of computer virus

b) Information about other data, such as the time and location it was created

c) A social media platform

d) A video game console

b) Information about other data, such as the time and location it was created.

In data protection, what does the
"right to data portability" mean?
Imagine it's like being able to move
your music playlist from one app to
another without losing anything. Can
you explain it more simply?

a) The right to carry a laptop everywhere

b) The right to request a copy of your personal
data in a common machine-readable format

c) The right to delete all your online accounts

d) The right to share any data you find online

b) The right to request a copy of your personal data in
a common machine-readable format.

In terms of keeping your messages private, what does "end-to-end encryption" mean? It's like sending a secret letter that only the recipient can open.

a) A method to ensure everyone can read a message

b) A way to hide messages from the recipient

c) A secure method of transmitting messages that only the sender and recipient can decrypt

d) A method to increase message latency

c) A secure method of transmitting messages that only the sender and recipient can decrypt.

In the world of privacy and security, what do people mean by a "threat model"? Think of it like creating a plan to keep your secrets safe online, kind of like deciding how to lock your front door at home.

a) A model for predicting the future of the internet

b) A model to determine potential risks and vulnerabilities to one's privacy and security

c) A mathematical model used in data analysis

d) A model for predicting the stock market

b) A model to determine potential risks and vulnerabilities to one's privacy and security.

In terms of keeping data safe and sound, what is "data encryption"?

a) Converting data into a human-readable format

b) Hiding data from authorized users

c) Encoding data to make it unreadable without the correct decryption key

d) Storing data on the cloud

c) Encoding data to make it unreadable without the correct decryption key.

The General Data Protection Regulation (GDPR) is a European law that protects information. What kind of information does it protect?

a) All information that somehow relates to a person

b) Only information that is digitalised

c) Only information that can be used to harm a person

d) Only information that relates to our health, ethnicity, religion, or political opinion

a) All information that somehow relates to a person .

European Data Protection law aims to protect our fundamental rights. Which other objective does it pursue?

a) facilitate the free flow of data

b) limit the free flow of data

c) prevent that data is stored outside of the EU

d) ensure that consumer are paid a fair price for their data

a) Facilitate the free flow of data.

Imagine a company that uses our data violates European data protection law. What is the maximum penalty it risks to receive?

a) Max. 100.000.000€

b) up to 4 % of the total worldwide annual turnover

c) The total value of data that has been processed unlawfully, multiplied by 10

d) Each country can determine the maximum amount of fines for themselves

b) up to 4 % of the total worldwide annual turnover.

Which of the following statements is false?

a) Data protection law regulates under which conditions companies can process and use our data

b) Data protection law prohibits companies from scanning the content of our private mails

c) Data protection law does not apply in personal (for example family) activities

d) The application of Data protection law is not dependent on the geographical establishment from businesses

b) Data protection law prohibits companies from scanning the content of our private mails.

The concept of 'informational self-determination' refers to...

a) the right to determine which information is correct or false

b) the capability of machines to take automated decisions

c) the right of an individual to decide which personal information is communicated to others

d) the right not to be subject to an automated decision by an algorithm

c) the right of an individual to decide which personal information is communicated to others.

Imagine a social media company wants to use the data it collects when you use its services. Is it allowed to do so without asking for your consent?

a) Yes, as long as they process data on another legal basis

b) Yes, but only if they proces data that cannot harm consumer

c) Yes, but only if they process data for non-commercial purposes

c) No, companies always have to obtain consent for the processing of our data

a) Yes, as long as they process data on another legal basis.

Data Protection Law demands from companies that use a lot of personal data to create which type of position?

a) Security Officer

b) Privacy Officer

c) Data Protection Officer

d) Compliance Officer

c) Data Protection Officer.

Which of the following information is NOT considered as 'sensitive data' and therefore not subject to stronger protection under the European data protection law?

a) data that reveals the financial situation

b) health data

c) data revealing political opinions

d) data revealing religious beliefs

a) Data the reveals the financial situation.

Data protection by design obliges
companies to…

a) incorporate the protection of personal data
as a secondary consideration in product
design
b) design products that do not collect
consumer data
c) consider data protection from the beginning
when designing products or services
d) consider data protection as an afterthought
in development process of goods and services

c) consider data protection from the beginning when
designing products or services.

What is understood by "consent" in data protection law?

a) A formal letter of approval

b) A verbal agreement

c) A clear, affirmative action indicating agreement

d) A passive acknowledgment of terms and conditions

c) A clear, affirmative action indicating agreement.

The 'privacy shield' was...

a) a protective cover for personal data

b) a legal framework that enabled data

transfers between the EU and the US

c) a new type of privacy fencing for homes

d) a (technological) shield that protects

against online privacy breaches

b) a legal framework that enabled data transfers
between the EU and the US.

To whom does European data
protection law apply?

a) only businesses

b) only businesses and public authorities

c) to everyone who processes digitalised
information

d) to everyone who processes personal data

d) to everyone who processes personal data.

Imagine a popular airline realises that criminals got access to all their passenger data (including payment details by consumers). Within which time frame does the company have to report this leak to authorities?

a) 24 hours after becoming aware of it

b) 72 hours after becoming aware of it

c) 1 week after becoming aware of it

d) 1 month after becoming aware of it

b) 72 hours after becoming aware of it.

The General Data Protection Regulation (GDPR) is a European Union regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. What action should companies take to comply under the GDPR?

a) By paying a fee to the supervisory authority

b) By appointing a Data Protection Officer (DPO)

c) By refusing to collect any user data

d) By ignoring the regulations altogether

b) By appointing a Data Protection Officer (DPO).

Violations of GDPR can have profound negative impacts on the entities responsible for data processing, like eroding trust, damaging reputation, and leading to legal consequences. What is the maximum fine for General Data Protection Regulation (GDPR) violations, expressed as a percentage of annual global turnover?

a) 1% of annual global turnover

b) 2% of annual global turnover

c) 4% of annual global turnover

d) 10% of annual global turnover

c) 4% of annual global turnove.

Under the General Data Protection Regulation (GDPR), which legal basis permits data processing without consent given by the data subject when processing is for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject?

a) Legitimate interest under GDPR Article 6(1)(f)

b) Consent under GDPR Article 6(1)a)

c) Legal obligation under GDPR Article 6(1)c)

d) Contractual necessity under GDPR Article 6(1)b)

d) Contractual necessity under GDPR Article 6(1)b).

What is the primary goal of the Digital Services Act?

a) Contributing to the proper functioning of the internal market for intermediary services

b) Protecting user privacy and security

c) Encouraging the growth of big tech companies

d) Reducing taxation on digital services

a) Contributing to the proper functioning of the internal market for intermediary services.

The Digital Services Act (DSA) addresses various aspects of online platforms, including their responsibilities, user rights, and the handling of data. Regarding data protection and user consent, what is the stance of the DSA?

a) It does not address data protection

b) It allows platforms to use user data without consent

c) It strengthens data protection and requires user consent

d) It bans the collection of user data

c) It strengthens data protection and requires user consent.

Personal data which belongs to individuals is collected by many companies , however, there are some ethical considerations to keep in mind while collecting this data. What are such ethical considerations?

a)   Obtaining informed consent from participants

b)   Protecting the privacy and confidentiality of participants' data

c)   Being transparent about the purpose of data collection and how the data will be used

d)   All of the above

d) All of the above.

Personal data protection laws allow for companies, businesses and persons to collect the personal data of their users only for specific and legitimate reasons. Whhich of the following is not a legitimate reason for a business to collect personal data?

a) To improve customer service

b) To develop new products and services

c) To target customers with personalized marketing messages

d) To sell the data to third-party companies without the customer's consent

---

d) To sell the data to third-party companies without the customer's consent.

There are various privacy preservation technologies in use across the world. Which of the following is an example of such privacy preservation technologies?

a) Intelligent Tracking Prevention

b) Enhanced Tracking Protection

c) Total Cookie Protection

d) All of the above

d) All of the above.

Which of the following is a new privacy technology that is being used to improve the security of online payments?

a) Tokenization

b) End-to-end encryption

c) Homomorphic encryption

d) All of the above

d) All of the above.

Data protection laws encourage technology companies collecting personal data of individuals to ensure that their technical systems are constructed in a way which protects the privacy of their users, this is broadly understood as privacy by design. Which of the following is NOT a principle of privacy by design?

a) Proactive not reactive; preventative not remedial

b) Privacy as the default setting

c) Full functionality – positive-sum, not zero-sum

d) Full transparency and openness

d) Full transparency and openness.

The General Data Protection Regulation also known as the GDPR is the primary legislation for protection of personal data in the European Union. What year was the regulation enacted?

a) 2015

b) 2019

c) 2017

d) 2018

d) 2018

The GDPR is a regulation in the EU focused on upholding privacy and protecting personal data. What is the full form of the GDPR?

a) General Data Privacy Regulation

b) General Data Protection Regulation

c) General Data Preservation Rules

d) General Data Protection Rules

b) General Data Protection Regulation.

Fundamental rights are extended towards protecting the personal data of individuals. Which of the following are NOT fundamental rights under the EU Charter of fundamental rights?

a) Protection of personal data

b) Non-discrimination

c) Respect for private and family life

d) Right of equality of personal and non-personal data

d) Right of equality of personal and non-personal data.

EU laws on data protection encourage member states to create regulatory sandboxes as an effort to engage with the companies processing personal data. What is a regulatory sandbox?

a) A controlled environment where businesses can test new products or services with real users without having to comply with all applicable regulations.

b) A government-run program that provides financial support to businesses that are developing new technologies.

c) A voluntary initiative by regulators to work with businesses to develop and test new regulatory frameworks.

d) All of the above.

d) All of the above.

Standardization protocols are a set of
technical specifications that ensure the
interoperability of products and services.
How can standardization protocols be used
to preserve privacy?

a) By providing a common framework for
collecting, using, and sharing data.

b) By making it easier to anonymize and de-
identify data.

c) By making it easier to implement privacy-
preserving technologies, such as encryption
and differential privacy.

d) All of the above.

d) All of the above.

What are some steps that individuals can take to protect their privacy online?

a) Be mindful of the apps and websites that you share your personal data with

b) Read the privacy policies of apps and websites before using them

c) Use strong passwords and enable two-factor authentication

d) All of the above

d) All of the above.

The International Organization for Standardization or the ISO is a worldwide federation of national standards bodies. The ISO sets out various standards which are crucial for data protection and cybersecurity. What is the ISO 27000 series?

a) A set of international standards for information security management

b) A set of international standards for data privacy

c) A set of international standards for cloud security

d) All of the above

a) A set of international standards for information security management.

The ISO 27001 is a set of international standards for information security management. What are the benefits of ISO 27001 certification?

a) Improved information security

b) Increased customer and partner confidence

c) Reduced risk of cyber attacks

d) All of the above

d) All of the above.

The International Organization for Standardization or the ISO is a worldwide federation of national standards bodies. The ISO sets out various standards which are crucial for data protection and cybersecurity. What is the ISO 27002 standard?

a) A code of practice for information security controls

b) A risk assessment methodology

c) A business continuity planning methodology

d) None of the above

d) None of the above.

What is a privacy architecture?

a) A framework for managing the privacy risks associated with information systems

b) A set of policies and procedures for protecting the privacy of personal data

c) A technical solution for encrypting and anonymizing personal data

d) All of the above

a) A framework for managing the privacy risks associated with information systems.

What is de-identification?

a) Enhancing data security

b) Removing personally identifiable information

c) Encrypting data at rest

d) Conducting data analysis

b) Removing personally identifiable information.

"De-identification" is the general term for the process of removing personal information from a record or data set. Which of the following is an example of personally identifiable information (PII)?

a) IP address

b) Bank account number

c) ID number

d) All of the above

d) All of the above.

Privacy

"De-identification" is the general term for the process of removing personal information from a record or data set. What does k-anonymity aim to achieve in de-identification?

a) Anonymizing all data

b) Ensuring each record has at least k quasi-identifiers

c) Removing all sensitive data

d) Encrypting the entire dataset

b) Ensuring each record has at least k quasi-identifiers.

"De-identification" is the general term for the process of removing personal information from a record or data set. What is the primary objective of de-identification techniques?

a) Protecting data from cyberattacks

b) Preserving the privacy of individuals

c) Enhancing data accuracy

d) Speeding up data processing

b) Preserving the privacy of individuals.

"De-identification" is the general term for the process of removing personal information from a record or data set. Which deidentification technique replaces sensitive data with a consistent, unique identifier?

a) Data masking

b) Data obfuscation

c) Data pseudonymization

d) Data anonymization

c) Data pseudonymization.

"De-identification" is the general term for the process of removing personal information from a record or data set. What is the primary drawback of deidentification techniques?

a) Reduced data utility

b) Increased data security

c) Enhanced data accuracy

d) Faster data retrieval

a) Reduced data utility.

The UK government has been accused of not doing enough to protect the country from cyber attacks.

a) True

b) False

a) True.

The European Data Protection Board (EDPB) is an independent European body established in 2018 to ensure the consistent application of the General Data Protection Regulation (GDPR) and to promote cooperation among the national data protection authorities (DPAs) of the European Economic Area (EEA)

a) True

b) False

a) True.

True or False: If you want to know which information companies are holding about you, companies are obliged to provide that data to you.

a) True
b) False

a) True.