

Name: _____

Date: _____

Score: _____

Data Privacy Standards & Global Compliance

Data privacy laws (GDPR, CCPA), encryption at-rest and in-transit, data minimization practices

DATA PRIVACY STANDARDS LEARNING OVERVIEW

SECURED

DATA ENCRYPTION

256-bit AES Standard

COMPLIANT

GLOBAL STANDARDS

GDPR & CCPA Frameworks

ZERO-TRUST

ACCESS POLICY

Multi-Factor Authentication

Welcome! This activity packet guides you through global data privacy standards. You will explore GDPR opt-in consent, CCPA opt-out sales rights, data minimization practices, full-disk encryption at rest, and TLS transit.

WORKSHEET CHECKPOINTS

- ☐ **Part 1-4:** Master cybersecurity and threat prevention.
- ☐ **Part 5-7:** Solve crossword & word search puzzles.
- ☐ **Part 8-9:** Solve case studies & cipher challenge.
- ☐ **Part 10:** Review basic & advanced FAQ pages.
- ☐ **Part 11:** Explore 10 interesting real-world facts.

Open the VPN.com Cybersecurity Guide

URL: <https://www.vpn.com/cybersecurity/data-privacy/>

Your Data Compliance & Privacy Learning Roadmap

- Understand compliance standards under GDPR and CCPA regulations.
- Implement data encryption controls for assets at rest and in transit.
- Formulate data minimization practices to reduce breach exposure.
- Establish active opt-in consent pathways for corporate websites.
- Apply cryptographic shredding keys to safely purge historical backup tapes.

DATA PRIVACY GUIDE INSTRUCTIONS

Answer the multiple choice and true/false questions, complete the fill-in-the-blank sentences using the word bank, match definitions, and solve the crossword and word search puzzles. Apply your knowledge to global data compliance.

DATA PRIVACY STANDARDS & REGULATORY COMPLIANCE (INTRODUCTION)

Data privacy defines how personal information is collected, processed, and secured. Complying with regulatory frameworks (like GDPR and CCPA) requires data minimization, explicit user consent models, encryption at-rest, and secure TLS transit protocols.

READ EACH CHECKPOINT CAREFULLY AND SELECT OR WRITE THE CORRECT RESPONSE.

Checkpoint 1: Multiple Choice Challenge

1 What is the core principle of GDPR data minimization?

- ☐ A. Collecting only data necessary for stated purposes
- ☐ B. Compressing databases to save system storage
- ☐ C. Restricting data viewing to corporate executives
- ☐ D. Encrypting traffic using protocol certificates

2 Which mechanism protects data stored on local database drives?

- ☐ A. Implementing full-disk encryption at rest
- ☐ B. Using virtual private network data tunneling
- ☐ C. Restricting registry nameserver cached entries
- ☐ D. Changing domain names to secure extensions

3 Under GDPR, what constitutes a valid user consent model?

- ☐ A. Active, opt-in choice with clear intent documentation
- ☐ B. Pre-checked option boxes on registration forms
- ☐ C. Continued website browsing without explicitly opting out
- ☐ D. Hiding the privacy agreement inside page source code

4 How does CCPA differ from GDPR in consumer rights?

- ☐ A. CCPA focus is on opt-out rights for data sales
- ☐ B. CCPA restricts data encryption standards globally
- ☐ C. CCPA applies only to public government databases
- ☐ D. CCPA is enforced by ICANN registry lock audits

5 Which protocol secures data packets moving across networks?

- ☐ A. Transport Layer Security encryption in transit
- ☐ B. Domain Name System nameserver lookup tables
- ☐ C. Uniform Resource Locator parameter parsing
- ☐ D. Extensible Provisioning Protocol authorization codes

Checkpoint 2: True or False Challenge

6 Question tf1

Data privacy and data security mean the same thing.

☐ True ☐ False

7 Question tf2

GDPR compliance applies to any company targeting EU residents.

☐ True ☐ False

8 Question tf3

Data encrypted at rest is safe from SQL injection exploits.

☐ True ☐ False

9 Question tf4

Minimizing data storage reduces the financial impact of breaches.

☐ True ☐ False

10 Question tf5

CCPA allows users to opt out of the sale of personal data.

☐ True ☐ False

Checkpoint 3: Key Term Insertion

Read each sentence below and fill in the blank with the correct term from the Word Bank.

1. Aligning practices with GDPR rules ensures regulatory _____.
2. Obtaining explicit opt-in choice represents active _____.
3. Storing only the minimum required user records is data _____.
4. Protecting database assets on storage drives requires encryption _____.
5. HTTPS protocols secure user sessions and data in _____.
6. Data governance rules focus on protecting individual _____.

VOCABULARY WORD BANK

PRIVACY
TRANSIT

SECURITY
ATREST

MINIMIZATION
COMPLIANCE

ENCRYPTION
CONSENT

Write your answers here:

- | | | | |
|----|----------------------|----|----------------------|
| 1. | <input type="text"/> | 2. | <input type="text"/> |
| 3. | <input type="text"/> | 4. | <input type="text"/> |
| 5. | <input type="text"/> | 6. | <input type="text"/> |

Checkpoint 4: Security Concept Match

DEFINITION MATCHING

Match each vocabulary term on the left with its correct definition on the right by writing the corresponding letter (A-H) in the fillable input box.

1. GDPR Regulation

A

European regulatory framework governing personal data protection.

2. CCPA Law

B

California state privacy law enforcing opt-out rights for data sales.

3. Data Minimizing

C

Limiting record collection to the absolute necessary minimum.

4. Storage At-Rest

D

Encrypting saved databases on local system storage drives.

5. Network Transit

E

Encrypting moving network packets using TLS certificates.

6. User Consent

F

Active, explicit opt-in agreement from web users.

7. Data Compliance

G

Aligning organizational data operations with global laws.

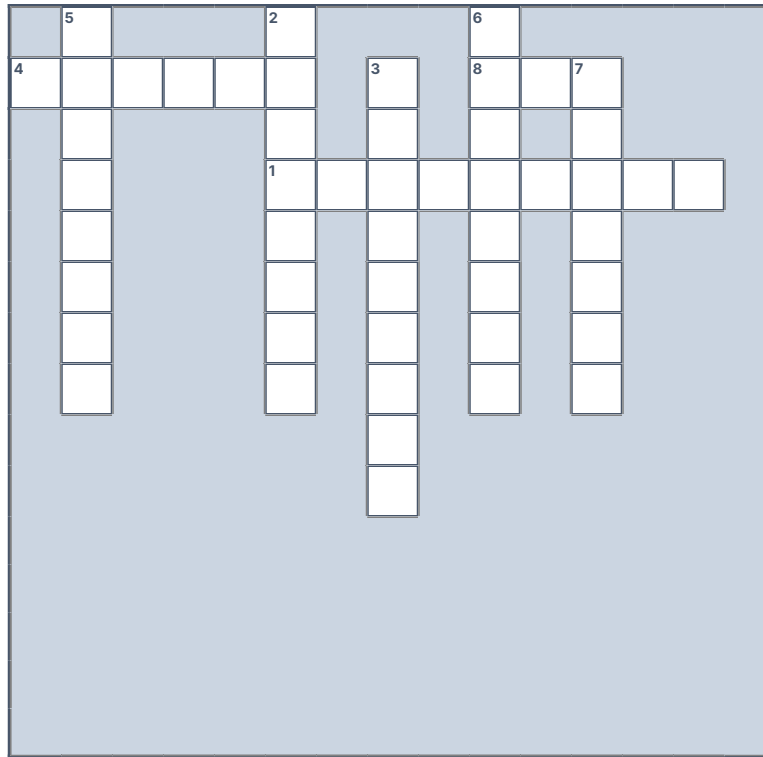
8. Privacy Shield

H

Safeguarding user privacy through structured data governance.

Checkpoint 5: Crossword Puzzle

Solve the crossword puzzle by typing letters into the active white boxes. The numbers correspond to the clues below.



ACROSS

1. Process of wrapping data packets inside other packets (9)
4. Remote server that routes traffic and hides your IP (6)
8. Internet Service Provider, logs traffic unless encrypted (3)

DOWN

2. Rules determining how data is sent and encrypted (8)
3. Rate of data transfer across a path (9)
5. Blocking site access based on location (8)
6. Security system that monitors and blocks traffic (8)
7. State of being free from tracking or surveillance (7)

Checkpoint 5 Alternative: Accessible Crossword Clues

Screen-reader and keyboard users can type the crossword answers directly in the text fields below.

ACROSS CLUES

1 Across: Wrapping data packets inside secure transport protocols. (9 letters):

4 Across: Network node acting as hosting anchor for virtual links. (6 letters):

8 Across: ISP gateway provider controlling endpoint routing links. (3 letters):

DOWN CLUES

2 Down: Standard formatting protocol governing online transmissions. (8 letters):

3 Down: Total transmission volume processed through physical links. (9 letters):

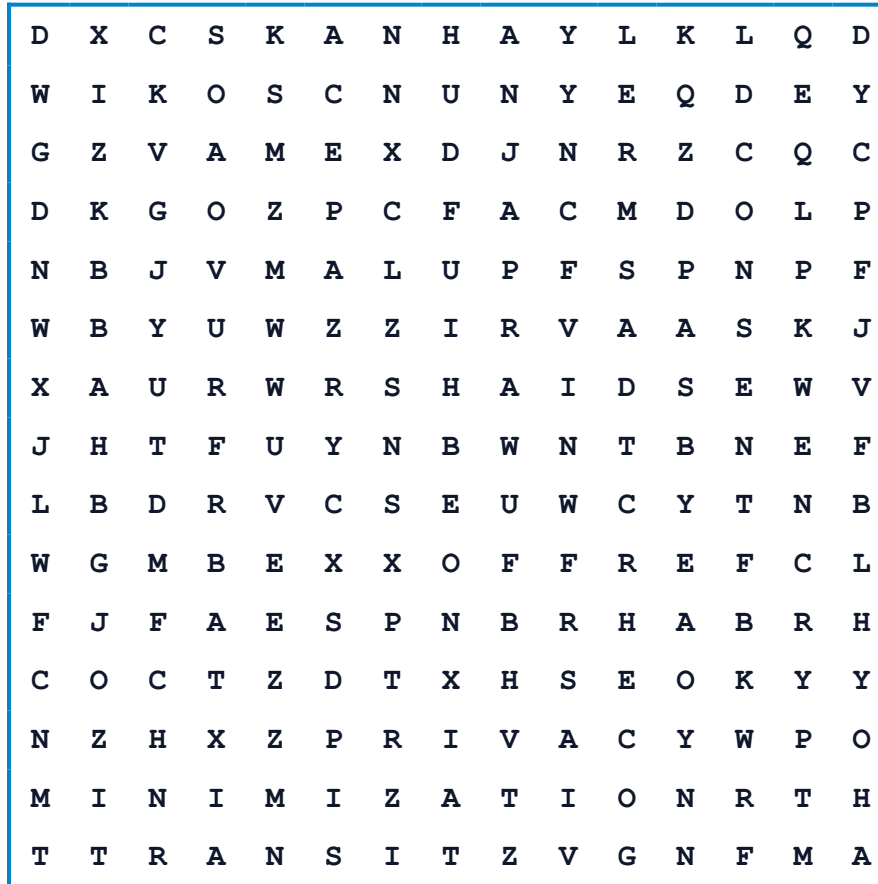
5 Down: Restricting resource availability by tracking geographic IP ranges. (8 letters):

6 Down: Intrusion protection system filtering local traffic segments. (8 letters):

7 Down: Confidential asset state shielded from public exposure. (7 letters):

Checkpoint 6: Hidden Word Search

Find the 8 key vocabulary terms hidden in the grid below. Words can be horizontal, vertical, or diagonal.



VOCABULARY WORD LIST

PRIVACY
ATREST

SECURITY
CONSENT

MINIMIZATION
COMPLIANCE

TRANSIT
ENCRYPT

Checkpoint 6 Alternative: Accessible Vocabulary Matching

Match each of the 8 vocabulary terms from the Word Search to its correct definition by writing the letter (A-H) in the blank space.

VOCABULARY TERMS

- A. PRIVACY
- B. SECURITY
- C. MINIMIZATION
- D. TRANSIT
- E. ATREST
- F. CONSENT
- G. COMPLIANCE
- H. ENCRYPT

DEFINITIONS & MATCH FIELDS

- ☐ 1. European regulatory framework governing personal data protection.
- ☐ 2. California state privacy law enforcing opt-out rights for data sales.
- ☐ 3. Limiting record collection to the absolute necessary minimum.
- ☐ 4. Encrypting saved databases on local system storage drives.
- ☐ 5. Encrypting moving network packets using TLS certificates.
- ☐ 6. Active, explicit opt-in agreement from web users.
- ☐ 7. Aligning organizational data operations with global laws.
- ☐ 8. Safeguarding user privacy through structured data governance.

Checkpoint 7: Scrambled Word Challenge

Unscramble the letters below to reveal key cybersecurity concepts and terms. Write your answers in the input boxes provided.

1. C Y I V A R P

5. T S E R T A

2. T Y I R U C E S

6. E N S O N C T

3. T I O N A Z I M I N I M

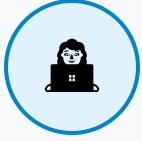
7. C E N A I L P M O C

4. T I S N A R T

8. T Y R C E N P

Checkpoint 8: Cybersecurity Case Studies

Apply the concepts you have learned to solve the real-world scenarios below.



CASE STUDY 1: COMPLIANCE WITH GDPR ERASURE

Scenario: A former client contacts an online platform demanding the deletion of all their personal records under GDPR's Right to Erasure. The platform has user records spread across operational databases and cold storage backups.

Discussion Question: Explain the compliance obligations and outline a secure remediation plan.



CASE STUDY 2: DATA MINIMIZATION AUDIT

Scenario: A startup collects user birthdates, zip codes, and phone numbers to send newsletter updates. They run a data privacy audit.

Discussion Question: Evaluate why this collection violates data minimization principles, and describe the remediation.

Final Challenge: Decrypting the Cipher

A cybersecurity professional protects network assets from online threat actors. Use the Letter-to-Number key below to decrypt the message by writing the matching letters in the blank spaces.

LETTER-TO-NUMBER ENCRYPTION KEY

A=1	B=2	C=3	D=4	E=5	F=6	G=7	H=8	I=9	J=10	K=11	L=12	M=13
N=14	O=15	P=16	Q=17	R=18	S=19	T=20	U=21	V=22	W=23	X=24	Y=25	Z=26

$\frac{\quad}{16}$	$\frac{\quad}{18}$	$\frac{\quad}{15}$	$\frac{\quad}{20}$	$\frac{\quad}{5}$	$\frac{\quad}{3}$	$\frac{\quad}{20}$	$\frac{\quad}{16}$	$\frac{\quad}{5}$	$\frac{\quad}{18}$	$\frac{\quad}{19}$	$\frac{\quad}{15}$	$\frac{\quad}{14}$	$\frac{\quad}{1}$	$\frac{\quad}{12}$			
$\frac{\quad}{4}$	$\frac{\quad}{1}$	$\frac{\quad}{20}$	$\frac{\quad}{1}$	$\frac{\quad}{23}$	$\frac{\quad}{9}$	$\frac{\quad}{20}$	$\frac{\quad}{8}$	$\frac{\quad}{18}$	$\frac{\quad}{15}$	$\frac{\quad}{2}$	$\frac{\quad}{21}$	$\frac{\quad}{19}$	$\frac{\quad}{20}$				
$\frac{\quad}{3}$	$\frac{\quad}{15}$	$\frac{\quad}{13}$	$\frac{\quad}{16}$	$\frac{\quad}{12}$	$\frac{\quad}{9}$	$\frac{\quad}{1}$	$\frac{\quad}{14}$	$\frac{\quad}{3}$	$\frac{\quad}{5}$	$\frac{\quad}{3}$	$\frac{\quad}{15}$	$\frac{\quad}{14}$	$\frac{\quad}{20}$	$\frac{\quad}{18}$	$\frac{\quad}{15}$	$\frac{\quad}{12}$	$\frac{\quad}{19}$

Decoded cybersecurity message:

TIP: EACH NUMBER REPRESENTS THE POSITION OF THAT LETTER IN THE ALPHABET (E.G. 1 = A, 2 = B, 26 = Z).

Checkpoint 10: Basic Cybersecurity FAQs (Part A)

Review common questions and answers regarding online threat mitigation.

Q1: What is the difference between data privacy and data security?

Data privacy governs who has authorized access to personal records, while data security protects data from unauthorized hackers and leaks.

Q2: What is GDPR?

GDPR is the European Union's General Data Protection Regulation, enforcing strict rules on personal data collection and user privacy rights.

Q3: What is CCPA?

CCPA is the California Consumer Privacy Act, granting consumers rights to know what data is collected and opt out of its sale.

Q4: What does data minimization mean?

It is the privacy practice of collecting and processing only the personal records strictly necessary to perform a specified task.

Q5: How is data encrypted at rest?

At-rest encryption protects stored databases on hard drives, using cryptographic keys to prevent reading if drives are stolen.

Checkpoint 10: Basic Cybersecurity FAQs (Part B)

Review common questions and answers regarding online threat mitigation.

Q6: How is data encrypted in transit?

In-transit encryption uses protocols like HTTPS/TLS to encrypt data packets as they move across network links, blocking packet sniffing.

Q7: What is the Right to Erasure?

Also known as the right to be forgotten, it allows users to demand organizations delete their personal data under specific rules.

Q8: What represents valid opt-in consent?

Opt-in consent is a clear, affirmative action by a user (like checking an unselected checkbox) indicating agreement to data processing.

Q9: Why is hashing passwords critical?

Hashing converts passwords into fixed-length cryptographic strings, preventing cleartext recovery if the database is breached.

Q10: What is a data privacy impact assessment (DPIA)?

A DPIA is an audit process used to identify and minimize privacy risks in new software development and database projects.

Checkpoint 11: Advanced Security FAQs (Part A)

Explore advanced technical aspects of security frameworks, malware analysis, and data compliance.

Q1: How does cryptographic shredding delete backup data?

Shredding deletes the encryption keys used to encrypt specific user files on backups, rendering the data permanently unrecoverable.

Q2: What is the role of a Data Protection Officer (DPO)?

A DPO is an independent compliance officer supervising an organization's data privacy strategy and ensuring GDPR regulatory alignment.

Q3: How do cookies impact GDPR compliance?

Cookies tracking user behavior represent personal data. Websites must obtain opt-in consent before setting tracking cookies on browsers.

Q4: What is the privacy risk of third-party trackers?

Trackers share user behavior across websites, often violating privacy laws if data is sent without explicit user disclosure and consent.

Q5: How does anonymization differ from pseudonymization?

Anonymization permanently alters data so users cannot be identified, while pseudonymization replaces identifiers with codes, allowing re-identification with key access.

Checkpoint 11: Advanced Security FAQs (Part B)

Explore advanced technical aspects of security frameworks, malware analysis, and data compliance.

Q6: What is the CCPA 'Do Not Sell' link requirement?

CCPA requires businesses to provide a clear 'Do Not Sell My Personal Information' link on homepage portals for easy opt-out.

Q7: How do global companies handle cross-border data transfers?

Companies use Standard Contractual Clauses (SCCs) and privacy frameworks to ensure data sent abroad meets original jurisdiction rules.

Q8: How does SQL injection expose encrypted drives?

SQL injection runs database queries through application APIs. Since the database is running, it automatically decrypts stored records, bypassing drive encryption.

Q9: What is privacy by design?

It is an engineering standard requiring security and privacy controls to be integrated into systems from the initial design phase, not added post-launch.

Q10: What are the maximum financial penalties under GDPR?

Violations can result in fines up to 20 million Euros or 4% of the organization's global annual revenue, whichever is higher.

Part 11: 10 Real-World Cybersecurity Facts & Insights

Review real-world facts regarding security breaches, defense mechanisms, and compliance standards.

1. SECURITY INSIGHT

GDPR regulations took effect in May 2018, changing how global sites manage cookie consents and personal data registries.

2. SECURITY INSIGHT

A GDPR violation fine can reach 20 million Euros or 4% of global turnover, representing substantial legal exposure.

3. SECURITY INSIGHT

The CCPA went into effect in January 2020, establishing pioneering digital privacy consumer rights in the United States.

4. SECURITY INSIGHT

Data minimization reduces database storage footprint, cutting server operating costs while decreasing breach impact scales.

5. SECURITY INSIGHT

Cryptographic shredding solves the backup deletion challenge by purging keys rather than editing historical backup tape files.

6. SECURITY INSIGHT

Over 70% of countries globally have enacted personal data protection laws to protect consumer privacy rights.

7. SECURITY INSIGHT

Opt-in consent forms with pre-checked boxes are explicitly banned under European data privacy regulatory definitions.

8. SECURITY INSIGHT

GDPR mandates that organizations report severe network data breaches to authorities within 72 hours of discovery.

9. SECURITY INSIGHT

Hashing passwords with bcrypt or Argon2 algorithms prevents reverse-engineering cracking attempts by threat actors.

10. SECURITY INSIGHT

Data at rest represents saved database files, while data in transit covers packets actively moving across network routers.

Technical References & Sources

The study guide and interactive puzzles are compiled from global NIST, OWASP, and data privacy compliance standards.

SCHOLARLY & INDUSTRY REFERENCES

- [1] CISA. (2025). Cybersecurity Alerts & Advisories. Retrieved from <https://www.cisa.gov/news-events/cybersecurity-advisories>
- [2] GDPR. (2024). General Data Protection Regulation (GDPR) Official Text. Retrieved from <https://gdpr-info.eu/>
- [3] NIST. (2024). Special Publication 800-53: Security and Privacy Controls. Retrieved from <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
- [4] NIST. (2023). Special Publication 800-61: Computer Security Incident Handling Guide. Retrieved from <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>
- [5] NIST. (2023). Special Publication 800-88: Guidelines for Media Sanitization. Retrieved from <https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final>
- [6] IETF. (2021). RFC 8446: Transport Layer Security (TLS) 1.3 Specification. Retrieved from <https://datatracker.ietf.org/doc/rfc8446/>
- [7] IETF. (2022). RFC 7519: JSON Web Token (JWT) Specification. Retrieved from <https://datatracker.ietf.org/doc/rfc7519/>
- [8] Center for Internet Security (CIS). (2024). Critical Security Controls. Retrieved from <https://www.cisecurity.org/controls/cis-controls-list>
- [9] OWASP. (2024). Top 10 Web Application Security Risks. Retrieved from <https://owasp.org/www-project-top-ten/>
- [10] OWASP. (2025). Application Security Verification Standard (ASVS). Retrieved from <https://owasp.org/www-project-application-security-verification-standard/>

Answer Key: Checkpoint 1 - Multiple Choice

1 Data Minimization

MINIMIZATION

Correct Answer: A

TEACHING NOTE

Data minimization restricts data collection to the absolute necessary minimum to limit breach exposure.

Citation: OWASP Secure Configuration [Ref 10].

2 Encryption At Rest

AT REST

Correct Answer: A

TEACHING NOTE

Full-disk encryption protects saved databases on hard drives from physical theft exploits.

Citation: NIST Digital Identity [Ref 9].

3 Opt-In Consent

GDPR CONSENT

Correct Answer: A

TEACHING NOTE

GDPR compliance requires active, explicit opt-in choice rather than pre-checked checkbox options.

Citation: Center for Internet Security (CIS) [Ref 8].

4 CCPA Rights

CCPA LAW

Correct Answer: A

TEACHING NOTE

CCPA enforces consumers' rights to opt out of the sale of personal information to third parties.

Citation: Center for Internet Security (CIS) [Ref 8].

5 Encryption In Transit

TRANSIT TLS

Correct Answer: A

TEACHING NOTE

HTTPS/TLS protocols encrypt session traffic, preventing credential sniffing on networks.

Citation: IETF RFC 3986 [Ref 6].

Answer Key: Checkpoint 2 - True or False

6 Privacy vs Security

PRIVACY

Correct Answer: False

TEACHING NOTE

Data privacy restricts user data access permissions, while security blocks malicious intrusions.

Citation: OWASP Secure Configuration [Ref 10].

7 GDPR Jurisdiction

GDPR COMPLIANCE

Correct Answer: True

TEACHING NOTE

GDPR governs any organization targeting EU users, regardless of corporate location.

Citation: Center for Internet Security (CIS) [Ref 8].

8 Injection Exploits

SQL INJECTION

Correct Answer: False

TEACHING NOTE

Full-disk encryption does not prevent SQL injections since the DB is decrypted when active.

Citation: NIST Digital Identity [Ref 9].

9 Minimizing Records

MINIMIZATION

Correct Answer: True

TEACHING NOTE

Reducing saved customer records minimizes the data size and financial exposure during breaches.

Citation: Center for Internet Security (CIS) [Ref 8].

10 Opt-Out Sales

CCPA LAW

Correct Answer: True

TEACHING NOTE

CCPA laws force sites to provide 'Do Not Sell' portals so consumers can block data sales.

Citation: Center for Internet Security (CIS) [Ref 8].

Vocabulary Keys & Grading Rubric

Instructor Grading Rubric: Award 1 point for each correct matching (8 points total) and context term (6 points total).

CHECKPOINT 4: CONCEPT MATCH KEY

A 1. GDPR Regulation

B 2. CCPA Law

C 3. Data Minimizing

D 4. Storage At-Rest

E 5. Network Transit

F 6. User Consent

G 7. Data Compliance

H 8. Privacy Shield

CHECKPOINT 3: KEY TERM KEY

1 COMPLIANCE

2 CONSENT

3 MINIMIZATION

4 ATREST

5 TRANSIT

6 PRIVACY

DISCUSSION NOTES FOR INSTRUCTORS

Threat Landscape:

Verify that students understand how malware, phishing, and zero-day attacks target and disrupt network defenses.

Defense Controls:

Emphasize the deployment of network firewalls, sandbox execution, behavior scanners, and multi-factor authentication (MFA).

Regulatory Compliance:

Highlight user consent, data minimization, encryption at-rest and in-transit, and global frameworks like GDPR/CCPA.

Puzzles Keys & Instructor Notes

WORD SEARCH SOLUTION

D	X	C	S	K	A	N	H	A	Y	L	K	L	Q	D
W	I	K	O	S	C	N	U	N	Y	E	Q	D	E	Y
G	Z	V	A	M	E	X	D	J	N	R	Z	C	Q	C
D	K	G	O	Z	P	C	F	A	C	M	D	O	L	P
N	B	J	V	M	A	L	U	P	F	S	P	N	P	F
W	B	Y	U	W	Z	Z	I	R	V	A	A	S	K	J
X	A	U	R	W	R	S	H	A	I	D	S	E	W	V
J	H	T	F	U	Y	N	B	W	N	T	B	N	E	F
L	B	D	R	V	C	S	E	U	W	C	Y	T	N	B
W	G	M	B	E	X	X	O	F	F	R	E	F	C	L
F	J	F	A	E	S	P	N	B	R	H	A	B	R	H
C	O	C	T	Z	D	T	X	H	S	E	O	K	Y	Y
N	Z	H	X	Z	P	R	I	V	A	C	Y	W	P	O
M	I	N	I	M	I	Z	A	T	I	O	N	R	T	H
T	T	R	A	N	S	I	T	Z	V	G	N	F	M	A

CROSSWORD SOLUTION

					</									

INSTRUCTOR GUIDE FOR CROSSWORD SOLUTIONS

ACROSS CLUES

- 1 Across:** **TUNNELING** Process of wrapping data packets. (3, 5)
- 4 Across:** **SERVER** Remote computer routing traffic. (1, 0)
- 8 Across:** **ISP** Internet Service Provider. (1, 9)

DOWN CLUES

- 2 Down:** **PROTOCOL** Rules determining data transmission. (0, 5)
- 3 Down:** **BANDWIDTH** Rate of data transfer. (1, 7)
- 5 Down:** **GEOBLOCK** Location website restriction. (0, 1)
- 6 Down:** **FIREWALL** Security monitor barrier. (0, 9)
- 7 Down:** **PRIVACY** State of freedom from tracking. (1, 11)

Scrambled Words & Cipher Solution Key

Grading key for the vocabulary word unscramble activity and Secret Cipher Challenge.

WORD UNSCRAMBLE KEY

1. C Y I V A R P

PRIVACY

5. T S E R T A

ATREST

2. T Y I R U C E S

SECURITY

6. E N S O N C T

CONSENT

3. T I O N A Z I M I N I M

MINIMIZATION

7. C E N A I L P M O C

COMPLIANCE

4. T I S N A R T

TRANSIT

8. T Y R C E N P

ENCRYPT

SECRET CIPHER CHALLENGE KEY

**"PROTECT PERSONAL DATA WITH ROBUST COMPLIANCE
CONTROLS"**

Domain Brokerage Case Studies Solution Key

A Case Study 1: Compliance with GDPR Erasure

[Instructor Solution](#)

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** A former client contacts an online platform demanding the deletion of all their personal records under GDPR's Right to Erasure. The platform has user records spread across operational databases and cold storage backups.
- **Recommended Strategy & Solution:** Obligations: The platform must erase all personal data within 30 days of the request. Remediation: 1. Delete user files from active databases. 2. If deletion from backups is technically impossible, cryptographically shred the specific user decryption keys, rendering the backup data permanently unreadable. 3. Log compliance actions.

B Case Study 2: Data Minimization Audit

[Instructor Solution](#)

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** A startup collects user birthdates, zip codes, and phone numbers to send newsletter updates. They run a data privacy audit.
- **Recommended Strategy & Solution:** Violation: Collecting birthdates and phone numbers is unnecessary for sending newsletter updates. It increases identity theft exposure in a breach. Remediation: Purge historical phone and birthdate fields, update signup forms to request email addresses only, and update the privacy policy.