Nume: _____ **Data:** _____ **Punctaj:** _____

Protejarea datelor personale și Drepturile tale

Date personale, drepturi de confidențialitate (GDPR, CCPA), brokeri de date, cookie-uri, phishing, VPN-uri și conturi mai sigure

PREZENTARE GENERALĂ DESPRE CONFIDENȚIALITATEA DATELOR PERSONALE

INFORMAT
CUNOAȘTE-ȚI DATELE
Ce se colectează și de ce

ÎMPUTERNICIT
DREPTURI DE CONFIDENȚIALITATE
Drepturile GDPR și CCPA/CPRA

VIGILANT
OBICEIURI INTELIGENTE
MFA, actualizări și recunoașterea escrocheriilor

Bun venit! Acest pachet de activități te ajută să preiei controlul asupra datelor tale personale. Vei explora drepturile la confidențialitate conform GDPR și CCPA, brokerii de date, consimțământul pentru cookie-uri, permisiunile aplicațiilor, phishing-ul, Wi-Fi-ul public, VPN-urile și MFA.

PUNCTE DE CONTROL ALE FIȘEI DE LUCRU

- [ ] **Partea 1-4: Învață-ți drepturile de confidențialitate și obiceiurile sigure.**
- [ ] **Partea 5-7: Rezolvă puzzle-uri de tip cuvinte încrucișate și căutare de cuvinte.**
- [ ] **Partea 8-9: Rezolvă studii de caz și provocarea cu codul cifrat.**
- [ ] **Partea 10: Parcurge paginile de întrebări frecvente de bază și avansate.**
- [ ] **Partea 11: Explorează 10 fapte interesante din lumea reală.**
- [ ] **Bonus: provocarea Gândește repede.**

Deschide Ghidul VPN.com despre confidențialitatea datelor

URL: https://www.vpn.com/ro/securitate-cibernetica/confidentialitatea-datelor/

Harta ta de învățare despre confidențialitatea datelor personale

- Înțelege-ți drepturile la confidențialitate conform GDPR și CCPA din California.
- Recunoaște cum colectează date personale brokerii de date, modulele cookie și aplicațiile.
- Aplică minimizarea datelor, împărtășind doar ceea ce are cu adevărat nevoie un serviciu.
- Fă alegeri informate la bannerele de cookie-uri și la solicitările de permisiuni ale aplicațiilor.
- Reduce riscul din phishing, breșe de securitate și Wi-Fi public cu MFA și actualizări.

INSTRUCȚIUNI PENTRU GHIDUL DE CONFIDENȚIALITATE A DATELOR

Răspunde la întrebările cu alegere multiplă și adevărat/fals, completează propozițiile cu spații libere folosind banca de cuvinte, asociază definițiile și rezolvă cuvintele încrucișate și puzzle-ul de căutare a cuvintelor. Aplică ce ai învățat despre protejarea propriilor tale date personale. Încheie cu activitatea bonus Gândește repede.

CONFIDENȚIALITATEA DATELOR PERSONALE ȘI DREPTURILE TALE (INTRODUCERE)

Confidențialitatea datelor este capacitatea ta de a controla modul în care informațiile tale personale sunt colectate, folosite, stocate și partajate. Legi precum GDPR și CCPA îți conferă drepturi, iar obiceiuri precum parolele puternice, MFA și partajarea atentă pot ajuta la reducerea riscului.

CITEȘTE ATENT FIECARE PUNCT DE CONTROL ȘI ALEGE SAU SCRIE RĂSPUNSUL CORECT.

Punct de control 1: Provocare cu alegere multiplă

1. Care alegere reflectă cel mai bine principiul minimizării datelor?

- A. Partajarea doar a datelor de care are nevoie un serviciu pentru scopul său
- B. Acordarea accesului complet fiecărei aplicații pentru a simplifica configurarea
- C. Completarea fiecărui câmp opțional din formularele de înscriere
- D. Reutilizarea unei singure parole pentru ca administrarea conturilor să fie mai ușoară

2. Ce pas este recomandat dacă un site pe care îl folosești raportează o breșă de securitate?

- A. Schimbă acea parolă și activează MFA acolo unde este oferită
- B. Refolosirea aceleiași parole pe un cont nou
- C. Răspunde la e-mailul despre breșă cu PIN-ul tău
- D. Ignoră-l, deoarece breșele rareori contează

3. Conform normelor UE, care este un consimțământ valid pentru cookie-urile de urmărire?

- A. Bifarea activă a unei căsuțe nebifate după o informare clară
- B. Casete bifate în prealabil pe un banner de cookie-uri sau de înscriere
- C. Continuarea simplă a derulării sau a navigării pe site
- D. O notificare ascunsă în termenii și condițiile site-ului

4. Ce drept au consumatorii din California în temeiul CCPA?

- A. Pentru a renunța la vânzarea sau partajarea datelor lor
- B. Pentru a fi plătit cu o taxă fixă pentru fiecare cerere de date
- C. Pentru a cere eliminarea oricărei aplicații din magazinele de aplicații
- D. Pentru a bloca orice colectare de date de către orice companie

5. Ce face în principal un VPN atunci când te conectezi la o rețea Wi-Fi publică?

- A. Criptează traficul dintre dispozitivul tău și serverul VPN
- B. Împiedică site-urile web să seteze orice cookie-uri
- C. Înlocuiește necesitatea MFA
- D. Elimină malware-ul aflat deja pe un dispozitiv

Punct de control 2: Provocare Adevărat sau Fals

6 Întrebare adevărat/fals 6

6. Confidențialitatea datelor și securitatea datelor înseamnă același lucru.

- ○ Adevărat
- ○ Fals

7 Întrebare adevărat/fals 7

7. GDPR se poate aplica și firmelor din afara UE care oferă servicii persoanelor din UE.

- ○ Adevărat
- ○ Fals

8 Întrebare adevărat/fals 8

8. Folosirea unui VPN împiedică site-urile web să te urmărească cu cookie-uri.

- ○ Adevărat
- ○ Fals

9 Întrebare adevărat/fals 9

9. Partajarea online a mai puține date personale poate reduce prejudiciul unei breșe de securitate.

- ○ Adevărat
- ○ Fals

10 Întrebare adevărat/fals 10

10. CCPA le permite consumatorilor să refuze vânzarea sau partajarea datelor lor.

- ○ Adevărat
- ○ Fals

Punct de control 3: Inserarea termenilor-cheie

Citește fiecare propoziție de mai jos și completează spațiul liber cu termenul corect din Banca de cuvinte.

1. Conform GDPR, _____ trebuie să fie dat liber, specific, informat și lipsit de ambiguitate, deci căsuțele bifate în prealabil nu contează.

2. Un _____ compilează detalii din registre publice, aplicații și achiziții pentru a construi și a vinde profiluri ale persoanelor.

3. Un mesaj text care pretinde că coletul tău este reținut și îți cere să „confirmi" datele cardului este o tentativă tipică de _____ .

4. HTTPS folosește _____ pentru a ajuta la protejarea datelor în tranzit între browser și un site web.

5. Împărtășirea doar a detaliilor de care un formular de înscriere are cu adevărat nevoie aplică principiul de _____ a datelor.

6. Dreptul la _____ îți permite să ceri unei organizații să îți șteargă datele personale, deși se aplică excepții.

BANCĂ DE CUVINTE DIN VOCABULAR

BROKER DE DATE CONSIMȚĂMÂNT COOKIE CRIPTARE MINIMIZARE PHISHING RENUNȚARE ȘTERGERE

Scrie răspunsurile aici:

1. _____ **2.** _____

3. _____ **4.** _____

5. _____ **6.** _____

Punct de control 4: Asocierea conceptelor despre confidențialitate

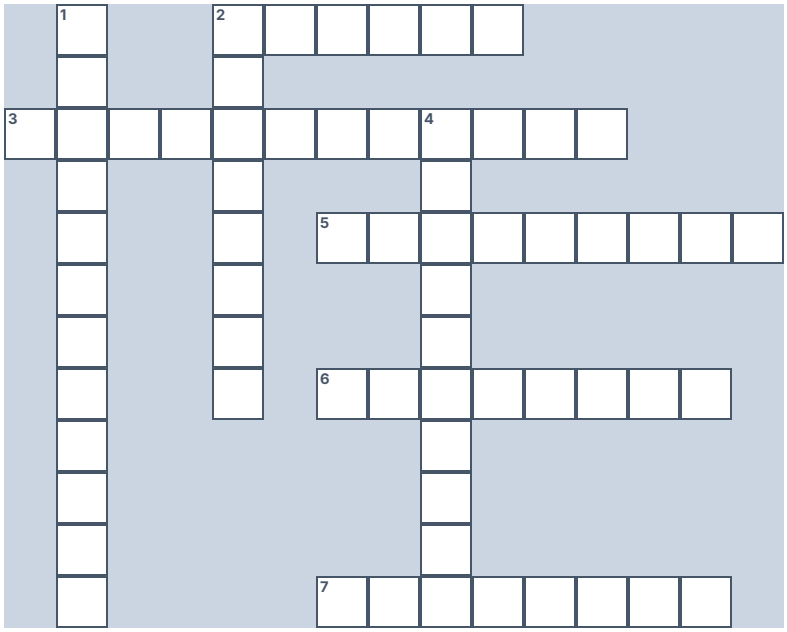
ASOCIEREA DEFINIȚIILOR

Asociază fiecare termen de vocabular din stânga cu definiția corectă din dreapta, scriind litera corespunzătoare (A-H) în câmpul de completare.

☐	1. Dreptul la ștergere	A	Dreptul din California de a opri o companie să îți vândă sau să îți partajeze datele.
☐	2. Dreptul de renunțare (opt-out)	B	Dreptul prevăzut de GDPR de a-ți șterge datele personale, sub rezerva unor excepții.
☐	3. Minimizarea datelor	C	Fișier mic din browser folosit pentru a-ți urmări activitatea pe site-uri web.
☐	4. Criptare	D	Acord liber exprimat, specific, informat și lipsit de ambiguitate.
☐	5. Broker de date	E	Colectarea doar a datelor personale necesare pentru un scop declarat.
☐	6. Consimțământ	F	Mesaje false care păcălesc oamenii să dezvăluie date sau date de autentificare.
☐	7. Phishing	G	Amestecarea datelor astfel încât doar cine are cheia potrivită să le poată citi.
☐	8. Cookie de urmărire	H	Firmă care compilează și vinde profiluri personale din multe surse.

Punct de control 5: Careu de cuvinte încrucișate

Rezolvă careul de cuvinte încrucișate tastând litere în căsuțele albe active. Numerele corespund indiciilor de mai jos.



ORIZONTAL

2. Mic fișier din browser care îți poate urmări activitatea pe mai multe site-uri (6)

3. Acord liber exprimat, specific, informat și lipsit de ambiguitate pentru utilizarea datelor (12)

5. Drept CCPA de a opri vânzarea sau partajarea datelor tale (9)

6. Mesaje false care te păcălesc să dezvălui autentificările sau datele cardului (8)

7. Drept care îți permite să ceri unei organizații să îți șteargă datele personale (8)

VERTICAL

1. Companie care compilează și vinde profiluri despre persoane (12)

2. Codificarea datelor astfel încât să le poată citi doar cine are cheia potrivită (8)

4. Minimizarea datelor: colectarea doar a ceea ce este necesar pentru un scop declarat (10)

Punct de control 5, variantă alternativă: Indicii accesibile pentru cuvinte încrucișate

Utilizatorii de cititoare de ecran și de tastatură pot introduce răspunsurile la cuvintele încrucișate direct în câmpurile de text de mai jos.

ORIZONTAL

2 orizontal: Mic fișier din browser care îți poate urmări activitatea pe mai multe site-uri (6 litere):

3 orizontal: Acord liber exprimat, specific, informat și lipsit de ambiguitate pentru utilizarea datelor (12 litere):

5 orizontal: Drept CCPA de a opri vânzarea sau partajarea datelor tale (9 litere):

6 orizontal: Mesaje false care te păcălesc să dezvălui autentificările sau datele cardului (8 litere):

7 orizontal: Drept care îți permite să ceri unei organizații să îți șteargă datele personale (8 litere):

VERTICAL

1 vertical: Companie care compilează și vinde profiluri despre persoane (12 litere):

2 vertical: Codificarea datelor astfel încât să le poată citi doar cine are cheia potrivită (8 litere):

4 vertical: Minimizarea datelor: colectarea doar a ceea ce este necesar pentru un scop declarat (10 litere):

Punct de control 6: Căutarea cuvintelor ascunse

Găsește în grila de mai jos cei 8 termeni cheie de vocabular ascunși. Cuvintele pot fi orizontale, verticale sau diagonale.

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

LISTĂ DE CUVINTE DIN VOCABULAR

ȘTERGERE RENUNȚARE MINIMIZARE CRIPTARE BROKERDEDATE
CONSIMȚĂMÂNT PHISHING COOKIE

Punct de control 6, variantă alternativă: Asocierea accesibilă a vocabularului

Asociază fiecare dintre cei 8 termeni de vocabular din Căutarea de cuvinte cu definiția corectă, scriind litera (A-H) în spațiul liber.

TERMENI DE VOCABULAR

- **A. ȘTERGERE**
- **B. RENUNȚARE**
- **C. MINIMIZARE**
- **D. CRIPTARE**
- **E. BROKERDEDATE**
- **F. CONSIMȚĂMÂNT**
- **G. PHISHING**
- **H. COOKIE**

DEFINIȚII ȘI CÂMPURI DE ASOCIERE

_____ 1. Drept CCPA de a opri vânzarea sau partajarea datelor tale.

_____ 2. Acord liber exprimat, specific, informat și lipsit de ambiguitate pentru utilizarea datelor.

_____ 3. Companie care compilează și vinde profiluri despre persoane.

_____ 4. Drept care îți permite să ceri unei organizații să îți șteargă datele personale.

_____ 5. Minimizarea datelor: colectarea doar a ceea ce este necesar pentru un scop declarat.

_____ 6. Mesaje false care te păcălesc să dezvălui autentificările sau datele cardului.

_____ 7. Mic fișier din browser care îți poate urmări activitatea pe mai multe site-uri.

_____ 8. Codificarea datelor astfel încât să le poată citi doar cine are cheia potrivită.

Punct de control 7: Provocare cu cuvinte amestecate

Descifrează literele de mai jos pentru a dezvălui conceptele și termenii-cheie de securitate cibernetică. Scrie răspunsurile în casetele de introducere furnizate.

1. **RRGȘETEE**
2. **RIMIMEZAIN**
3. **BREDTDOREEAK**
4. **SNGIHPHI**
5. **ANEEȚURRN**
6. **REPACTRI**
7. **ĂMICOȚTÂNNMS**
8. **OECIKO**

Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

1	Pași de urmat după o breșă de date			
2	Aplicații care îți cer locația			
3	Setări de confidențialitate de verificat pe un telefon nou			
4	Semne că un calculator este infectat			
5	Semne că un mesaj ar putea fi phishing			
6	Motive pentru care ar trebui să actualizezi software-ul			
7	Detalii personale de ținut departe de rețelele sociale			
8	Moduri de a-ți proteja conturile			
9	Informații pe care nu ar trebui să le dai niciodată			
10	Conturi care ar trebui să aibă MFA activat			
11	Lucruri pe care le salvezi într-o copie de rezervă			
12	Locuri în care ai putea folosi Wi-Fi public			
13	Lucruri de făcut după o scurgere de date			
14	Companii care ar putea colecta datele tale de navigare			
15	Semnale de avertizare într-un e-mail			

Punct de control 8: Studii de caz despre confidențialitatea datelor

Aplică conceptele pe care le-ai învățat în scenariile reale de mai jos.

STUDIU DE CAZ 1: SOLICITAREA ȘTERGERII DATELOR DE PE UN SITE

👷

Scenariu: Maya, care locuiește în Franța, și-a închis contul de pe o aplicație de cumpărături acum doi ani, dar încă primește e-mailurile ei de marketing. Vrea ca aplicația să-i șteargă datele personale în baza dreptului la ștergere din GDPR.

Întrebare de discuție: Ce pași ar putea urma Maya și ce date ar putea păstra aplicația în mod legal?

STUDIU DE CAZ 2: O APLICAȚIE DE TESTE ȘI PERMISIUNILE

👷

Scenariu: O aplicație gratuită cu teste de personalitate îi cere lui Leo locația, contactele, microfonul și data nașterii înainte de a putea începe.

Întrebare de discuție: Ce permisiuni par inutile și ce opțiuni are Leo pentru a reduce cantitatea de informații pe care o partajează?

Punct de control 9: Descifrează codul

Persoanele atente la confidențialitate se opresc înainte de a-și partaja online datele personale. Folosește cheia Literă-Număr de mai jos pentru a descifra mesajul, scriind literele corespunzătoare în spațiile libere.

CHEIE DE CRIPTARE LITERĂ-NUMĂR

A=1 Ă=2 Â=3 B=4 C=5 D=6 E=7 F=8 G=9 H=10 I=11

Î=12 J=13 K=14 L=15 M=16 N=17 O=18 P=19 Q=20 R=21 S=22

Ș=23 T=24 Ț=25 U=26 V=27 W=28 X=29 Y=30 Z=31

9	3	17	6	7	23	24	7		12	17	1	11	17	24	7		22	2
	19	1	21	24	1	13	7	31	11		18	17	15	11	17	7		

Mesaj descifrat:

SFAT: FIECARE NUMĂR REPREZINTĂ POZIȚIA ACELEI LITERE ÎN ALFABET (DE EX. 1 = A, 2 = B, 31 = Z).

Punct de control 10: Întrebări frecvente de bază despre confidențialitatea datelor (Partea A)

Parcurge întrebările și răspunsurile frecvente despre protejarea datelor tale personale.

Q1: Care este diferența dintre confidențialitatea datelor și securitatea datelor?

Confidențialitatea este controlul tău asupra modului în care datele personale sunt colectate, folosite și partajate; securitatea este protecția care le ferește de accesul neautorizat.

Q2: Ce este GDPR?

Regulamentul general privind protecția datelor al UE, aplicabil din 25 mai 2018, stabilește reguli pentru prelucrarea datelor cu caracter personal și le oferă persoanelor drepturi asupra lor [1].

Q3: Ce este CCPA?

California Consumer Privacy Act, astfel cum a fost modificat prin CPRA, oferă rezidenților drepturile de a cunoaște, șterge, corecta și refuza vânzarea sau partajarea datelor [4].

Q4: Ce înseamnă minimizarea datelor?

Folosirea doar a datelor cu caracter personal adecvate, relevante și limitate la ceea ce este necesar pentru un scop; ca utilizator, o poți aplica partajând mai puțin [1].

Q5: Ce sunt permisiunile aplicațiilor?

Setări care permit aplicațiilor să acceseze locația, contactele sau fotografiile tale; verificarea lor și dezactivarea celor inutile poate limita colectarea de date [8].

Punct de control 10: Întrebări frecvente de bază despre confidențialitatea datelor (Partea B)

Parcurge întrebările și răspunsurile frecvente despre protejarea datelor tale personale.

Q6: Ce face HTTPS pentru confidențialitatea mea?

HTTPS criptează datele dintre browserul tău și un site, dar și site-urile de înșelătorie pot folosi HTTPS, deci lacătul nu dovedește că un site este de încredere [10].

Q7: Ce este dreptul la ștergere?

Potrivit articolului 17 din GDPR, poți cere unei organizații să îți șteargă datele în anumite cazuri; dreptul nu este absolut și are excepții [1].

Q8: Ce se consideră consimțământ valid?

Un act afirmativ clar, precum bifarea unei căsuțe nebifate în prealabil, după o informare clară; căsuțele prebifate, tăcerea sau derularea paginii nu contează [2].

Q9: Ce face o parolă puternică?

Lungimea contează cel mai mult: NIST cere site-urilor să impună cel puțin 15 caractere pentru parolele folosite singure și să permită managerii de parole [11].

Q10: Ce ar trebui să fac după o breșă de date?

Schimbă parolele afectate, activează MFA, monitorizează-ți conturile și ia în considerare un îngheț gratuit al creditului; IdentityTheft.gov enumeră pașii de recuperare [9].

Punct de control 10: Întrebări frecvente avansate despre confidențialitate (Partea C)

Explorează întrebări mai profunde despre bazele legale, cookie-uri, urmărire, brokerii de date și drepturile tale online.

Q1: Necesită orice prelucrare de date consimțământul meu conform GDPR?

Nu. Consimțământul este unul dintre cele șase temeiuri legale din articolul 6; altele includ contractul, obligația legală și interesele legitime [1].

Q2: Unde se aplică GDPR?

Organizațiilor stabilite în UE, precum și celor din afara UE care oferă bunuri sau servicii persoanelor din UE ori le monitorizează comportamentul [1].

Q3: Au nevoie site-urile de consimțământ pentru toate modulele cookie?

Nu întotdeauna. Cookie-urile strict necesare sunt în general scutite, dar cele neesențiale, precum cookie-urile de urmărire, necesită un consimțământ valid prealabil [3].

Q4: Care este riscul pentru confidențialitate al trackerelor terțe?

Trackerele terțe te pot urmări pe multe site-uri pentru a-ți afișa reclame direcționate; ștergerea cookie-urilor și ajustarea setărilor de confidențialitate pot ajuta [8].

Q5: Ce este un broker de date?

O companie care colectează informații personale din diverse surse și le vinde altor companii; rezidenții din California pot folosi platforma DROP a statului pentru a solicita ștergerea [5].

Punct de control 10: Întrebări frecvente avansate despre confidențialitate (Partea D)

Explorează întrebări mai profunde despre bazele legale, cookie-uri, urmărire, brokerii de date și drepturile tale online.

Q6: Ce este link-ul CCPA „Do Not Sell or Share”?

Companiile care vând sau partajează date trebuie, în general, să ofere un link „Do Not Sell or Share My Personal Information” și să respecte semnalele de renunțare precum GPC [4].

Q7: Mă face un VPN anonim?

Nu. Un VPN criptează traficul către serverul VPN și îți ascunde IP-ul față de site-uri, dar furnizorul îl poate vedea, iar cookie-urile și fingerprintingul te pot totuși urmări [12].

Q8: Cum pot recunoaște un mesaj de phishing?

Fii atent la solicitările urgente de a da clic pe link-uri, de a confirma datele de plată sau de a remedia probleme ale contului; contactează compania folosind un număr de telefon sau un site web despre care știi că este real [7].

Q9: Este sigur să folosesc Wi-Fi-ul public?

Poate fi riscant. Majoritatea site-urilor folosesc criptare, așa că verifică prezența HTTPS, ține software-ul actualizat și folosește MFA [10]; un VPN poate adăuga protecție în rețelele nesigure [12].

Q10: Care sunt sancțiunile financiare maxime conform GDPR?

Pentru cele mai grave încălcări, amenzile pot ajunge la 20 de milioane de euro sau la 4% din cifra de afaceri anuală la nivel mondial, oricare dintre acestea este mai mare [1].

Partea 11: 10 fapte și perspective din lumea reală despre confidențialitatea datelor

Parcurge fapte din lumea reală despre legile confidențialității, brokerii de date, fraude, breșe de securitate și obiceiuri online mai sigure.

1. INFORMAȚII DESPRE CONFIDENȚIALITATE

GDPR se aplică din 25 mai 2018 și le oferă persoanelor drepturi de acces, de corectare și de ștergere a datelor lor cu caracter personal [1].

2. INFORMAȚII DESPRE CONFIDENȚIALITATE

Conform GDPR, cele mai grave încălcări pot atrage amenzi de până la 20 de milioane de euro sau 4% din cifra de afaceri la nivel mondial [1].

3. INFORMAȚII DESPRE CONFIDENȚIALITATE

Modificările aduse prin CPRA la CCPA din California au intrat în vigoare la 1 ianuarie 2023 și au adăugat drepturi de corectare a datelor și de limitare a utilizării datelor sensibile [4].

4. INFORMAȚII DESPRE CONFIDENȚIALITATE

Potrivit FTC, consumatorii au raportat pierderi de 15,9 miliarde de dolari din cauza fraudelor în 2025, față de peste 12 miliarde de dolari în anul precedent [6].

5. INFORMAȚII DESPRE CONFIDENȚIALITATE

Din 1 ianuarie 2026, rezidenții din California pot folosi platforma gratuită DROP pentru a cere brokerilor de date să-și șteargă datele personale [5].

6. INFORMAȚII DESPRE CONFIDENȚIALITATE

Conform normelor UE privind protecția datelor, căsuțele bifate în prealabil, tăcerea sau inactivitatea nu constituie un consimțământ valid [2].

7. PERSPECTIVĂ ASUPRA CONFIDENȚIALITĂȚII

În Marea Britanie, site-urile trebuie să îți ofere o modalitate de a-ți exprima consimțământul pentru orice cookie care nu este strict necesar pentru site-ul web [3].

8. PERSPECTIVĂ ASUPRA CONFIDENȚIALITĂȚII

GDPR impune ca anumite încălcări ale securității datelor cu caracter personal să fie raportate autorității în termen de 72 de ore, acolo unde este fezabil [1].

9. PERSPECTIVĂ ASUPRA CONFIDENȚIALITĂȚII

NIST spune că site-urile nu ar trebui să impună schimbări periodice ale parolelor și ar trebui să verifice parolele noi în raport cu listele de parole compromise [11].

10. INFORMAȚII DESPRE CONFIDENȚIALITATE

Un VPN îți ascunde adresa IP față de site-uri web, dar furnizorul VPN îți poate vedea în continuare traficul, așa că alege cu atenție [12].

Referințe tehnice și surse

Ghidul de studiu și puzzle-urile se bazează pe ghidurile oficiale de confidențialitate ale UE, Regatului Unit, Californiei, FTC, NIST și EFF.

REFERINȚE OFICIALE ȘI DE SPECIALITATE

[1] European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union, L 119.

https://eur-lex.europa.eu/eli/reg/2016/679/oj

[2] European Data Protection Board. (2020). Guidelines 05/2020 on consent under Regulation 2016/679.

https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[3] Information Commissioner's Office. (n.d.). Cookies. ICO for the public.

https://ico.org.uk/for-the-public/online/cookies/

[4] California Privacy Protection Agency. (n.d.). Frequently asked questions (FAQs).

https://cppa.ca.gov/faq.html

[5] California Privacy Protection Agency. (2025). Delete Request and Opt-out Platform (DROP).

https://privacy.ca.gov/drop/

[6] Federal Trade Commission. (2026, March 25). FTC testifies before the Joint Economic Committee on agency's efforts to combat fraud [Press release].

https://www.ftc.gov/news-events/news/press-releases/2026/03/ftc-testifies-joint-economic-committee-agencys-efforts-combat-fraud

[7] Federal Trade Commission. (2022). How to recognize and avoid phishing scams. Consumer Advice.

https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

[8] Federal Trade Commission. (2023). How websites and apps collect and use your information. Consumer Advice.

https://consumer.ftc.gov/articles/how-websites-and-apps-collect-and-use-your-information

[9] Federal Trade Commission. (2024). What to know about identity theft. Consumer Advice.

https://consumer.ftc.gov/articles/what-know-about-identity-theft

[10] Federal Trade Commission. (2023). Are public Wi-Fi networks safe? What you need to know. Consumer Advice.

https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[11] National Institute of Standards and Technology. (2025). Digital identity guidelines: Authentication and authenticator management (NIST SP 800-63B-4).

https://csrc.nist.gov/pubs/sp/800/63/b/4/final

[12] Electronic Frontier Foundation. (2026). Choosing the VPN that's right for you. Surveillance Self-Defense.

https://ssd.eff.org/module/choosing-vpn-thats-right-you

Barem: Punct de control 1 – Alegere multiplă

1 **Minimizarea datelor** MINIMIZARE — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Articolul 5 din GDPR prevede că datele cu caracter personal trebuie să fie adecvate, relevante și limitate la ceea ce este necesar; utilizatorii pot imita acest principiu partajând mai puține date [1].

2 **Răspunsul la o breșă** BRESĂ — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

După o breșă, schimbă parolele expuse, activează MFA și monitorizează conturile; IdentityTheft.gov oferă pași de recuperare personalizați [9].

3 **Consimțământ valid** CONSIMȚĂMÂNTUL PENTRU COOKIE-URI — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Un consimțământ valid necesită un act afirmativ clar, după informare clară; căsuțele bifate în prealabil și derularea continuă nu se califică [2].

4 **Drepturi conform CCPA** LEGEA CCPA — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Consumatorii din California pot refuza vânzarea sau partajarea informațiilor personale, inclusiv prin semnalele Global Privacy Control [4].

5 **Protecție VPN** TUNEL VPN — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Un VPN criptează traficul către serverul VPN și îți ascunde IP-ul față de site-uri, dar cookie-urile și fingerprintingul te pot urmări în continuare [12].

Barem: Punct de control 2 – Adevărat sau fals

6 **Confidențialitate vs. securitate** CONFIDENȚIALITATE — **Răspuns corect: Fals**

NOTĂ PENTRU PROFESOR

Înrudite, dar diferite: articolul 5 din GDPR stabilește reguli privind modul de utilizare a datelor, în timp ce articolul 32 cere separat măsuri de securitate [1].

7 **Domeniul de aplicare teritorial al GDPR** DOMENIUL DE APLICARE AL GDPR — **Răspuns corect: Adevărat**

NOTĂ PENTRU PROFESOR

Articolul 3(2) acoperă organizațiile din afara UE care oferă bunuri sau servicii persoanelor din UE sau care monitorizează comportamentul acestora [1].

8 **VPN-uri și cookie-uri** LIMITELE VPN — **Răspuns corect: Fals**

NOTĂ PENTRU PROFESOR

Un VPN îți ascunde adresa IP, dar cookie-urile, pixelii de urmărire și fingerprintingul te pot urmări în continuare pe site-uri web [12].

9 **Partajarea mai puțină** MINIMIZARE — **Răspuns corect: Adevărat**

NOTĂ PENTRU PROFESOR

Dezactivarea permisiunilor inutile ale aplicațiilor și partajarea a mai puține date limitează ce poate fi colectat și expus ulterior într-o breșă [8].

10 **Renunțare la vânzarea sau partajarea datelor** LEGEA CCPA — **Răspuns corect: Adevărat**

NOTĂ PENTRU PROFESOR

Companiile care vând sau partajează date trebuie să ofere un link clar de renunțare, precum „Do Not Sell or Share My Personal Information” [4].

Chei de vocabular și grilă de notare

Barem de notare pentru profesor: Acordă 1 punct pentru fiecare asociere corectă (8 puncte în total) și pentru fiecare termen din context (6 puncte în total).

PUNCT DE CONTROL 4: BAREM – ASOCIEREA CONCEPTELOR

B 1. Dreptul la ștergere	A 2. Dreptul de renunțare (opt-out)	E 3. Minimizarea datelor	G 4. Criptare
H 5. Broker de date	D 6. Consimțământ	F 7. Phishing	C 8. Cookie de urmărire

PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

1 CONSIMȚĂMÂNT	2 BROKER DE DATE	3 PHISHING	4 CRIPTARE
5 MINIMIZARE	6 ȘTERGERE		

PUNCT DE CONTROL 6, VARIANTĂ ALTERNATIVĂ: BAREM – ASOCIEREA CUVINTELOR

1 B – RENUNȚARE	2 F – CONSIMȚĂMÂNT	3 E – BROKERDEDATE	4 A – ȘTERGERE
5 C – MINIMIZARE	6 G – PHISHING	7 H – COOKIE	8 D – CRIPTARE

NOTE DE DISCUȚIE PENTRU PROFESORI

Termeni-cheie:
Verifică dacă elevii pot explica Dreptul la ștergere, Dreptul de renunțare (opt-out) și Minimizarea datelor cu propriile cuvinte și pot da câte un exemplu pentru fiecare.

Studii de caz:
Cere elevilor să își susțină recomandările cu fapte din fișă, nu cu presupuneri.

Evaluarea surselor:
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

Chei de rezolvare ale puzzle-urilor și note pentru profesor

SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE

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

SOLUȚIA CUVINTELOR ÎNCRUCIȘATE

	B			C	O	O	K	I	E					
	R			R										
C	O	N	S	I	M	Ț	Ă	M	Â	N	T			
	K			P				I						
	E			T		R	E	N	U	N	Ț	A	R	E
	R			A				I						
	D			R				M						
	E			E		P	H	I	S	H	I	N	G	
	D							Z						
	A							A						
	T							R						
	E					Ș	T	E	R	G	E	R	E	

GHID PENTRU PROFESOR: SOLUȚIILE LA CUVINTELE ÎNCRUCIȘATE

ORIZONTAL

2 orizontal: COOKIE Mic fișier din browser care îți poate urmări activitatea pe mai multe site-uri (6 litere)

3 orizontal: CONSIMȚĂMÂNT Acord liber exprimat, specific, informat și lipsit de ambiguitate pentru utilizarea datelor (12 litere)

5 orizontal: RENUNȚARE Drept CCPA de a opri vânzarea sau partajarea datelor tale (9 litere)

6 orizontal: PHISHING Mesaje false care te păcălesc să dezvălui autentificările sau datele cardului (8 litere)

7 orizontal: ȘTERGERE Drept care îți permite să ceri unei organizații să îți șteargă datele personale (8 litere)

VERTICAL

1 vertical: BROKERDEDATE Companie care compilează și vinde profiluri despre persoane (12 litere)

2 vertical: CRIPTARE Codificarea datelor astfel încât să le poată citi doar cine are cheia potrivită (8 litere)

4 vertical: MINIMIZARE Minimizarea datelor: colectarea doar a ceea ce este necesar pentru un scop declarat (10 litere)

Cuvinte amestecate și barem pentru codul cifrat

Barem pentru activitatea de descifrare a cuvintelor de vocabular și pentru provocarea Codul secret.

BAREMUL PENTRU DESCIFRAREA CUVINTELOR

1. RRGȘETEE — ȘTERGERE
2. RIMIMEZAIN — MINIMIZARE
3. BREDTDOREEAK — BROKERDEDATE
4. SNGIHPHI — PHISHING
5. ANEEȚURRN — RENUNȚARE
6. REPACTRI — CRIPTARE
7. ĂMICOȚTÂNNMS — CONSIMȚĂMÂNT
8. OECIKO — COOKIE

BAREMUL PROVOCĂRII CU CODUL SECRET

"GÂNDEȘTE ÎNAINTE SĂ PARTAJEZI ONLINE"

Barem pentru studiile de caz

A Studiu de caz 1: Solicitarea ștergerii datelor de pe un site

Îndrumări pentru profesor

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: Maya, care locuiește în Franța, și-a închis contul într-o aplicație de cumpărături în urmă cu doi ani, dar încă primește e-mailurile de marketing ale acesteia. Ea vrea ca aplicația să-i șteargă datele personale în baza dreptului la ștergere prevăzut de GDPR.
- Abordări recomandate: Opțiunea 1: Maya trimite o cerere scrisă de ștergere și se opune marketingului direct, care trebuie apoi să înceteze; aplicația ar trebui, în general, să răspundă în termen de o lună [1]. Opțiunea 2: se dezabonează mai întâi pentru o ușurare rapidă. Motivare: ștergerea nu este absolută, așa că aplicația poate păstra datele necesare pentru obligații legale sau pretenții juridice [1]. Dacă nu răspunde, ea poate depune o plângere la autoritatea sa de protecție a datelor [1].

B Studiu de caz 2: O aplicație de teste și permisiunile

Îndrumări pentru profesor

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: O aplicație gratuită de teste de personalitate îi cere lui Leo locația, contactele, microfonul și data nașterii înainte de a putea începe.
- Abordări recomandate: Opțiunea 1: refuză accesul la locație, contacte și microfon, apoi verifică dacă testul funcționează în continuare [8]. Opțiunea 2: dacă aplicația insistă, alege o altă aplicație sau șterge-o [8]. Motivare: un test are rareori nevoie de acele date, iar partajarea a mai puține date limitează ce poate fi colectat, vândut sau expus. Leo poate, de asemenea, să verifice periodic permisiunile în setările de confidențialitate ale telefonului său [8].