Navn: _____ Dato: _____ Poeng: _____

Beskytte personopplysninger og Dine rettigheter

Personopplysninger, personvernrettigheter (GDPR, CCPA), databrokere, informasjonskapsler, nettfisking, VPN-er og tryggere kontoer

LÆRINGSOVERSIKT: PERSONVERN FOR PERSONOPPLYSNINGER

INFORMERT

KJENN DATAENE DINE

Hva som samles inn, og hvorfor

MYNDIGGJORT

PERSONVERNRETTIGHETER

Rettigheter under GDPR og CCPA/CPRA

VIGILANT

SMARTE VANER

MFA, oppdateringer og å oppdage svindel

Velkommen! Dette aktivitetsheftet hjelper deg med å ta kontroll over personopplysningene dine. Du utforsker personvernrettigheter under GDPR og CCPA, datameglere, samtykke til informasjonskapsler, apptillatelser, nettfisking, offentlig Wi-Fi, VPN-er og MFA.

KONTROLLPUNKTER I ARBEIDSARKET

- [ ] **Del 1-4: Lær om personvernrettighetene dine og trygge vaner.**
- [ ] **Del 5-7: Løs kryssord og ordsøk.**
- [ ] **Del 8-9: Løs casestudier og chifferutfordringen.**
- [ ] **Del 10: Gå gjennom sidene med grunnleggende og avanserte vanlige spørsmål.**
- [ ] **Del 11: Utforsk 10 interessante fakta fra virkeligheten.**
- [ ] **Bonus: Tenk raskt-utfordring.**

Åpne VPN.coms veiledning om personvern

URL: https://www.vpn.com/no/cybersikkerhet/datapersonvern/

Din læringsveiledning for personvern for personopplysninger

- Forstå personvernrettighetene dine etter GDPR og Californias CCPA.
- Forstå hvordan databrokere, informasjonskapsler og apper samler inn personopplysninger.
- Bruk dataminimering ved å dele bare det en tjeneste faktisk trenger.
- Ta informerte valg når du møter informasjonskapselbannere og forespørsler om apptillatelser.
- Reduser risikoen fra phishing, datainnbrudd og offentlig Wi-Fi med MFA og oppdateringer.

INSTRUKSJONER FOR PERSONVERNGUIDE

Svar på flervalgsspørsmålene og sant/usant-spørsmålene, fyll ut setningene med ordbanken, koble sammen definisjoner, og løs kryssordet og ordsøket. Bruk kunnskapen din på beskyttelse av dine egne personopplysninger. Avslutt med bonusaktiviteten Tenk raskt.

PERSONVERN FOR PERSONOPPLYSNINGER OG RETTIGHETENE DINE (INNLEDNING)

Personvern er muligheten din til å kontrollere hvordan personopplysningene dine samles inn, brukes, lagres og deles. Lover som GDPR og CCPA gir deg rettigheter, mens vaner som sterke passord, MFA og forsiktig deling kan bidra til å redusere risikoen.

LES HVERT KONTROLLPUNKT NØYE OG VELG ELLER SKRIV DET RIKTIGE SVARET.

Kontrollpunkt 1: Flervalgsutfordring

1. Hvilket valg gjenspeiler best prinsippet om dataminimering?

- A. Å dele bare de dataene en tjeneste trenger for sitt formål
- B. Å gi hver app full tilgang for å gjøre oppsettet enklere
- C. Å fylle ut hvert valgfrie felt i registreringsskjemaer
- D. Å gjenbruke ett passord slik at kontoer er enklere å administrere

2. Hvilket steg anbefales hvis et nettsted du bruker melder om et sikkerhetsbrudd?

- A. Endre det passordet og aktivere MFA der det tilbys
- B. Å gjenbruke samme passord på en ny konto
- C. Svar på e-posten om sikkerhetsbruddet med PIN-koden din
- D. Ignorer det, siden sikkerhetsbrudd sjelden betyr noe

3. Hva er gyldig samtykke til sporingsinformasjonskapsler etter EU-regler?

- A. Å aktivt krysse av i en boks som ikke var avkrysset, etter klar informasjon
- B. Forhåndsmerkede bokser i et banner for informasjonskapsler eller registrering
- C. Bare å fortsette å rulle eller surfe på nettstedet
- D. En melding skjult i nettstedets vilkår og betingelser

4. Hvilken rettighet har forbrukere i California under CCPA?

- A. Å velge bort salg eller deling av dataene sine
- B. Å få betalt et fast gebyr for hver dataforespørsel
- C. For å kreve at enhver app fjernes fra appbutikker
- D. For å blokkere all datainnsamling fra alle selskaper

5. Hva gjør et VPN først og fremst når du kobler til offentlig Wi-Fi?

- A. Krypterer trafikken mellom enheten din og VPN-serveren
- B. Hindrer nettsteder i å sette noen informasjonskapsler
- C. Den erstatter behovet for MFA
- D. Fjerner skadevare som allerede finnes på en enhet

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål (sant/usant) 6

6. Personvern og datasikkerhet betyr det samme.

○ Sant ○ Usant

7 Spørsmål (sant/usant) 7

7. GDPR kan gjelde for selskaper utenfor EU som tilbyr tjenester til personer i EU.

○ Sant ○ Usant

8 Spørsmål (sant/usant) 8

8. Å bruke en VPN hindrer ikke nettsteder i å spore deg med informasjonskapsler.

○ Sant ○ Usant

9 Spørsmål (sant/usant) 9

9. Å dele mindre personlig informasjon på nettet kan redusere skaden av et datainnbrudd.

○ Sant ○ Usant

10 Spørsmål (sant/usant) 10

10. CCPA lar forbrukere reservere seg mot salg eller deling av dataene sine.

○ Sant ○ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

Les hver setning nedenfor og fyll ut det tomme feltet med riktig begrep fra ordbanken.

1. I henhold til GDPR må _____ være fritt gitt, spesifikt, informert og utvetydig, så forhåndsavkryssede bokser teller ikke.

2. En _____ samler opplysninger fra offentlige registre, apper og kjøp for å bygge og selge profiler av personer.

3. En tekstmelding som hevder at pakken din er holdt tilbake og ber deg «bekrefte» kortopplysninger, er et typisk eksempel på _____ .

4. HTTPS bruker _____ for å bidra til å beskytte data på vei mellom nettleseren og et nettsted.

5. Å dele bare de opplysningene et registreringsskjema faktisk trenger, følger prinsippet om _____ .

6. Retten til _____ lar deg be en organisasjon slette personopplysningene dine, men det finnes unntak.

ORDBANK

COOKIE DATAMEGLER DATAMINIMERING FRAVALG KRYPTERING NETTFISKING SAMTYKKE SLETTING

Skriv svarene dine her:

1. **2.**

3. **4.**

5. **6.**

Kontrollpunkt 4: Koble personvernbegreper

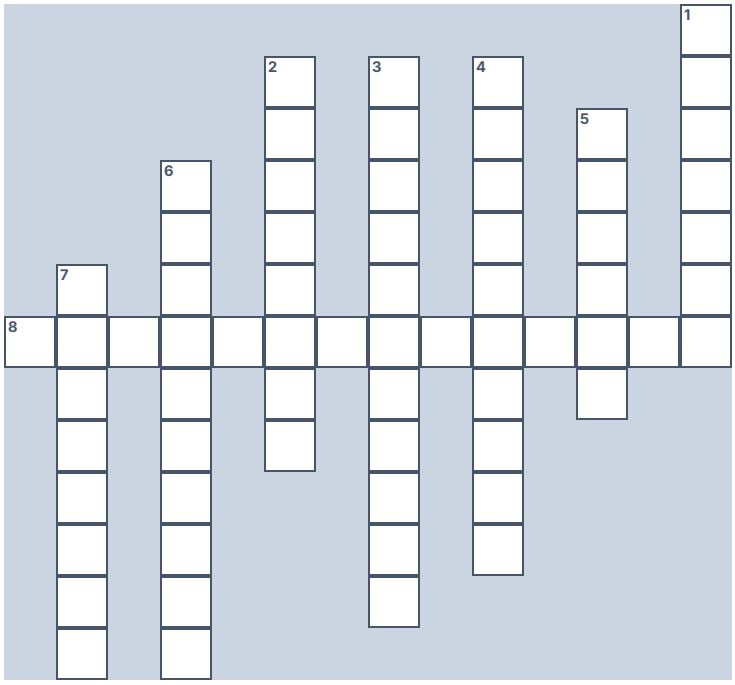
KOBLE DEFINISJONER

Koble hvert fagbegrep til venstre med riktig definisjon til høyre ved å skrive den tilhørende bokstaven (A-H) i det utfyllbare feltet.

☐	1. Retten til sletting	A	Retten i California til å stoppe en virksomhet fra å selge eller dele dataene dine.
☐	2. Rett til å reservere seg	B	Retten under GDPR til å få personopplysningene dine slettet, med forbehold om unntak.
☐	3. Dataminimering	C	Liten nettleserfil som brukes til å følge aktiviteten din på tvers av nettsteder.
☐	4. Kryptering	D	Fritt gitt, spesifikt, informert og utvetydig samtykke.
☐	5. Datamegler	E	Å samle inn bare de personopplysningene som trengs for et oppgitt formål.
☐	6. Samtykke	F	Falske meldinger som lurer folk til å avsløre data eller påloggingsopplysninger.
☐	7. Nettfisking	G	Å kryptere data slik at bare den som har riktig nøkkel, kan lese dem.
☐	8. Sporingsinformasjonskapsel	H	Firma som samler inn og selger personprofiler fra mange kilder.

Kontrollpunkt 5: Kryssord

Løs kryssordet ved å skrive bokstaver i de aktive hvite rutene. Tallene tilsvarer hintene nedenfor.



VANNRETT

8. Prinsippet om å samle inn bare det som trengs for et angitt formål (14)

LODDRETT

1. Rett etter CCPA til å stanse salg eller deling av dataene dine (7)

2. Rett som lar deg be en organisasjon slette personopplysningene dine (8)

3. Falske meldinger som lurer deg til å avsløre påloggінger eller kortopplysninger (11)

4. Å skramble data slik at bare den med riktig nøkkel kan lese dem (10)

5. Liten nettleserfil som kan følge aktiviteten din på tvers av nettsteder (6)

6. Selskap som samler og selger profiler om personer (10)

7. Fritt gitt, spesifikk, informert og utvetydig enighet om bruk av data (8)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

Brukere av skjermleser og tastatur kan skrive inn kryssordsvarene direkte i tekstfeltene nedenfor.

VANNRETT

8 vannrett: Prinsippet om å samle inn bare det som trengs for et angitt formål (14 bokstaver):

LODDRETT

1 loddrett: Rett etter CCPA til å stanse salg eller deling av dataene dine (7 bokstaver):

2 loddrett: Rett som lar deg be en organisasjon slette personopplysningene dine (8 bokstaver):

3 loddrett: Falske meldinger som lurer deg til å avsløre påloggінger eller kortopplysninger (11 bokstaver):

4 loddrett: Å skramble data slik at bare den med riktig nøkkel kan lese dem (10 bokstaver):

5 loddrett: Liten nettleserfil som kan følge aktiviteten din på tvers av nettsteder (6 bokstaver):

6 loddrett: Selskap som samler og selger profiler om personer (10 bokstaver):

7 loddrett: Fritt gitt, spesifikk, informert og utvetydig enighet om bruk av data (8 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

Finn de 8 sentrale ordforrådsbegrepene som er skjult i rutenettet nedenfor. Ordene kan stå vannrett, loddrett eller diagonalt.

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

ORDLISTE

SLETTING FRAVALG DATAMINIMERING KRYPTERING DATAMEGLER SAMTYKKE NETTFISKING COOKIE

Kontrollpunkt 6, alternativ: Tilgjengelig ordkobling

Koble hvert av de 8 fagbegrepene fra ordsøket til riktig definisjon ved å skrive bokstaven (A-H) i det tomme feltet.

BEGREPER
A. SLETTING
B. FRAVALG
C. DATAMINIMERING
D. KRYPTERING
E. DATAMEGLER
F. SAMTYKKE
G. NETTFISKING
H. COOKIE

DEFINISJONER OG TILHØRENDE FELT

_____ 1. Rett etter CCPA til å stanse salg eller deling av dataene dine.

_____ 2. Fritt gitt, spesifikk, informert og utvetydig enighet om bruk av data.

_____ 3. Selskap som samler og selger profiler om personer.

_____ 4. Rett som lar deg be en organisasjon slette personopplysningene dine.

_____ 5. Prinsippet om å samle inn bare det som trengs for et angitt formål.

_____ 6. Falske meldinger som lurer deg til å avsløre påloggінger eller kortopplysninger.

_____ 7. Liten nettleserfil som kan følge aktiviteten din på tvers av nettsteder.

_____ 8. Å skramble data slik at bare den med riktig nøkkel kan lese dem.

Kontrollpunkt 7: Utfordring med blandede ord

Sett bokstavene nedenfor sammen i riktig rekkefølge for å avsløre sentrale begreper innen cybersikkerhet. Skriv svarene dine i svarboksene.

1. NTTSILGE
2. MAITNNDIIGE RMA
3. DEEGAMRALT
4. SNGITFIKNET
5. AGVAFLR
6. NTPRIKREGY
7. SEYKKATM
8. OECIKO

Bonusaktivitet: Tenk raskt

3 SVAR PER KATEGORI. DEN SOM FYLLER UT LISTEN FØRST, VINNER.

1	Tiltak å ta etter et databrudd			
2	Apper som ber om posisjonen din			
3	Personverninnstillinger du bør gå gjennom på en ny telefon			
4	Tegn på at en datamaskin er infisert			
5	Tegn på at en melding kan være nettfiske			
6	Grunner til å oppdatere programvare			
7	Personlige opplysninger du bør holde unna sosiale medier			
8	Måter å beskytte kontoene dine på			
9	Informasjon du aldri bør dele			
10	Kontoer som bør ha MFA slått på			
11	Ting du tar sikkerhetskopi av			
12	Steder der du kan bruke offentlig Wi-Fi			
13	Ting å gjøre etter en datalekkasje			
14	Selskaper som kan samle inn nettleserdataene dine			
15	Advarselstegn i en e-post			

Kontrollpunkt 8: Casestudier om personvern

Bruk begrepene du har lært på de virkelige scenarioene nedenfor.

CASESTUDIE 1: BE ET NETTSTED OM Å SLETTE DATA



Scenario: Maya, som bor i Frankrike, avsluttet kontoen sin i en shoppingapp for to år siden, men får fortsatt markedsføringse-poster fra den. Hun vil at appen skal slette personopplysningene hennes i henhold til GDPRs rett til sletting.

Diskusjonsspørsmål: Hvilke skritt kan Maya ta, og hvilke data kan appen lovlig beholde?

CASESTUDIE 2: EN QUIZ-APP OG TILLATELSER



Scenario: En gratis personlighetsquiz-app ber Leo om posisjonen, kontaktene, mikrofonen og fødselsdatoen hans før han kan begynne.

Diskusjonsspørsmål: Hvilke tillatelser virker unødvendige, og hvilke muligheter har Leo for å redusere hvor mye han deler?

Kontrollpunkt 9: Knekk chifferet

Personvernbevisste mennesker stopper opp før de deler personlige opplysninger på nettet. Bruk bokstav-til-tall-nøkkelen nedenfor til å dekryptere meldingen ved å skrive de tilsvarende bokstavene i de tomme feltene.

NØKKEL FOR KRYPTERING AV BOKSTAV TIL TALL

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 Æ=27 Ø=28 Å=29

20	5	14	11		6	28	18		4	21		4	5	12	5	18		16	29

14	5	20	20

Dekodet melding:

TIPS: HVERT TALL REPRESENTERER BOKSTAVENS PLASS I ALFABETET (F.EKS. 1 = A, 2 = B, 29 = Å).

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om personvern (Del A)

Gå gjennom vanlige spørsmål og svar om beskyttelse av personopplysningene dine.

Q1: Hva er forskjellen mellom personvern og datasikkerhet?

Personvern er din kontroll over hvordan personopplysninger samles inn, brukes og deles; sikkerhet er beskyttelsen som hindrer uautorisert tilgang til dem.

Q2: Hva er GDPR?

EUs personvernforordning (GDPR), som gjelder fra 25. mai 2018, setter regler for behandling av personopplysninger og gir enkeltpersoner rettigheter over dem [1].

Q3: Hva er CCPA?

Californias Consumer Privacy Act, slik den er endret av CPRA, gir innbyggere rett til å få innsyn i, slette, rette og reservere seg mot salg eller deling av data [4].

Q4: Hva betyr dataminimering?

Å bruke bare personopplysninger som er tilstrekkelige, relevante og begrenset til det som er nødvendig for et formål; som bruker kan du anvende dette ved å dele mindre [1].

Q5: Hva er apptillatelser?

Innstillinger som gir apper tilgang til posisjon, kontakter eller bilder. Å gå gjennom dem og slå av dem du ikke trenger, kan begrense datainnsamlingen [8].

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om personvern (Del B)

Gå gjennom vanlige spørsmål og svar om beskyttelse av personopplysningene dine.

Q6: Hva gjør HTTPS for personvernet mitt?

HTTPS krypterer data mellom nettleseren din og et nettsted, men svindelnettsteder kan også bruke HTTPS, så hengelåsen beviser ikke at et nettsted er til å stole på [10].

Q7: Hva er retten til sletting?

Etter GDPR artikkel 17 kan du be en organisasjon om å slette dataene dine i visse tilfeller; retten er ikke absolutt og har unntak [1].

Q8: Hva regnes som gyldig samtykke?

En tydelig bekreftende handling, som å krysse av i en boks som ikke var avkrysset på forhånd, etter klar informasjon; forhåndsavkryssede bokser, stillhet eller rulling teller ikke [2].

Q9: Hva kjennetegner et sterkt passord?

Lengde betyr mest: NIST ber nettsteder om å kreve minst 15 tegn for passord som brukes alene, og om å tillate passordbehandlere [11].

Q10: Hva bør jeg gjøre etter et datainnbrudd?

Bytt berørte passord, slå på MFA, hold øye med kontoene dine og vurder en gratis kredittsperre. IdentityTheft.gov lister opp trinn for gjenoppretting [9].

Kontrollpunkt 10: Avanserte vanlige spørsmål om personvern (Del C)

Utforsk mer dyptgående spørsmål om rettslig grunnlag, informasjonskapsler, sporing, datameglere og rettighetene dine på nettet.

Q1: Krever all databehandling samtykke fra meg etter GDPR?

Nei. Samtykke er ett av seks lovlige grunnlag i artikkel 6; andre er blant annet avtale, rettslig forpliktelse og berettigede interesser [1].

Q2: Hvor gjelder GDPR?

Til organisasjoner etablert i EU, og til organisasjoner utenfor EU som tilbyr varer eller tjenester til, eller overvåker atferden til, personer i EU [1].

Q3: Trenger nettsteder samtykke for alle informasjonskapsler?

Ikke alltid. Strengt nødvendige informasjonskapsler er vanligvis unntatt, men ikke-essensielle, som sporingskapsler, krever forhåndssamtykke som er gyldig [3].

Q4: Hva er personvernrisikoen ved tredjepartssporere?

Tredjepartssporere kan følge deg på mange nettsteder for å vise målrettede annonser; å slette informasjonskapsler og justere personverninnstillingene kan hjelpe [8].

Q5: Hva er en databroker?

En virksomhet som samler inn personopplysninger fra ulike kilder og selger dem til andre selskaper; innbyggere i California kan bruke delstatens DROP-plattform til å be om sletting [5].

Kontrollpunkt 10: Avanserte vanlige spørsmål om personvern (Del D)

Utforsk mer dyptgående spørsmål om rettslig grunnlag, informasjonskapsler, sporing, datameglere og rettighetene dine på nettet.

Q6: Hva er CCPA-lenken «Do Not Sell or Share»?

Virksomheter som selger eller deler data må generelt tilby en lenke med teksten 'Do Not Sell or Share My Personal Information' og respektere signaler om reservasjon som GPC [4].

Q7: Gjør en VPN meg anonym?

Nei. En VPN krypterer trafikk til VPN-serveren og skjuler IP-adressen din for nettsteder, men leverandøren kan se den, og informasjonskapsler og fingeravtrykksporing kan fortsatt spore deg [12].

Q8: Hvordan kan jeg oppdage en nettfiskingsmelding (phishing)?

Vær oppmerksom på hastverkspregede oppfordringer om å klikke på lenker, bekrefte betalingsopplysninger eller løse kontoproblemer. Ta kontakt med selskapet via et telefonnummer eller en nettside du vet er ekte [7].

Q9: Er offentlig Wi-Fi trygt å bruke?

Det kan være risikabelt. De fleste nettsteder bruker kryptering, så sjekk at det er HTTPS, hold programvaren oppdatert og bruk MFA [10]. En VPN kan gi ekstra beskyttelse på upålitelige nettverk [12].

Q10: Hva er de høyeste økonomiske sanksjonene under GDPR?

For de mest alvorlige overtredelsene kan bøtene nå 20 millioner euro eller 4 % av global årlig omsetning, avhengig av hva som er høyest [1].

Del 11: 10 fakta om personvern fra virkeligheten og innsikt

Gå gjennom virkelighetsnære fakta om personvernlover, databrokere, svindel, datainnbrudd og tryggere vaner på nett.

1. PERSONVERNINNSIKT

GDPR har gjeldt siden 25. mai 2018 og gir folk rett til innsyn i, retting av og sletting av personopplysningene sine [1].

2. PERSONVERNINNSIKT

Etter GDPR kan de alvorligste bruddene gi bøter på opptil 20 millioner euro eller 4 % av global omsetning [1].

3. PERSONVERNINNSIKT

CPRA-endringene i Californias CCPA trådte i kraft 1. januar 2023 og la til rettigheter til å rette data og begrense bruken av sensitive data [4].

4. PERSONVERNINNSIKT

Forbrukere rapporterte å ha tapt 15,9 milliarder dollar til svindel i 2025, opp fra over 12 milliarder året før, ifølge FTC [6].

5. PERSONVERNINNSIKT

Siden 1. januar 2026 kan innbyggere i California bruke den gratis DROP-plattformen til å be datameglere om å slette personopplysningene deres [5].

6. PERSONVERNINNSIKT

Etter EUs personvernregler regnes forhåndsavkryssede bokser, stillhet eller passivitet ikke som gyldig samtykke [2].

7. PERSONVERNINNSIKT

I Storbritannia må nettsteder gi deg en måte å samtykke til alle informasjonskapsler som ikke er strengt nødvendige for nettstedet [3].

8. PERSONVERNINNSIKT

GDPR krever at visse brudd på personopplysningssikkerheten rapporteres til tilsynsmyndigheten innen 72 timer, der det er mulig [1].

9. PERSONVERNINNSIKT

NIST sier at nettsteder ikke bør tvinge fram periodiske passordbytter og bør sjekke nye passord mot lister over kompromitterte passord [11].

10. PERSONVERNINNSIKT

En VPN skjuler IP-adressen din for nettsteder, men VPN-leverandøren kan fortsatt se trafikken din, så velg nøye [12].

Tekniske referanser og kilder

Studieveiledningen og oppgavene bygger på offisiell veiledning om personvern fra EU, Storbritannia, California, FTC, NIST og EFF.

OFFISIELLE REFERANSER OG EKSPERTREFERANSER

[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

Fasit: Kontrollpunkt 1 – flervalg

1 **Dataminimering** MINIMERING **Riktig svar: A**

MERKNAD TIL LÆREREN

Artikkel 5 i GDPR krever at personopplysninger er adekvate, relevante og begrenset til det som er nødvendig. Brukere kan etterligne dette ved å dele mindre [1].

2 **Å reagere på et datainnbrudd** DATABRUDD **Riktig svar: A**

MERKNAD TIL LÆREREN

Etter et datainnbrudd bør du endre eksponerte passord, aktivere MFA og overvåke kontoer; IdentityTheft.gov tilbyr skreddersydde trinn for gjenoppretting [9].

3 **Gyldig samtykke** SAMTYKKE TIL INFORMASJONSKAPSLER **Riktig svar: A**

MERKNAD TIL LÆREREN

Gyldig samtykke krever en tydelig aktiv handling etter tydelig informasjon; forhåndsavkryssede bokser og fortsatt rulling gjelder ikke [2].

4 **CCPA-rettigheter** CCPA-LOVEN **Riktig svar: A**

MERKNAD TIL LÆREREN

Forbrukere i California kan reservere seg mot salg eller deling av personopplysninger, blant annet gjennom Global Privacy Control-signaler [4].

5 **VPN-beskyttelse** VPN-TUNNEL **Riktig svar: A**

MERKNAD TIL LÆREREN

En VPN krypterer trafikken til VPN-serveren og skjuler IP-adressen din for nettsteder, men infokapsler og fingeravtrykksporing kan fortsatt spore deg [12].

Fasit: Kontrollpunkt 2 – sant eller usant

6 **Personvern mot sikkerhet** PERSONVERN — **Riktig svar: Usant**

MERKNAD TIL LÆREREN

Beslektet, men forskjellig: GDPR artikkel 5 fastsetter regler for hvordan data brukes, mens artikkel 32 separat krever sikkerhetstiltak [1].

7 **GDPRs territorielle virkeområde** GDPR-VIRKEOMRÅDE — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Artikkel 3(2) omfatter organisasjoner utenfor EU som tilbyr varer eller tjenester til, eller overvåker atferden til, personer i EU [1].

8 **VPN-er og informasjonskapsler** GRENSER FOR VPN — **Riktig svar: Usant**

MERKNAD TIL LÆREREN

En VPN skjuler IP-adressen din, men infokapsler, sporingspiksler og fingeravtrykksporing kan fortsatt følge deg på tvers av nettsteder [12].

9 **Dele mindre** MINIMERING — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Å slå av unødvendige apptillatelser og dele mindre begrenser hva som kan samles inn og senere avsløres i et databrudd [8].

10 **Reserver deg mot salg eller deling** CCPA-LOVEN — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Virksomheter som selger eller deler data må tilby en tydelig lenke for reservasjon, for eksempel 'Do Not Sell or Share My Personal Information' [4].

Fasit for ordforråd og vurderingsmatrise

Rettemal for læreren: Gi 1 poeng for hver riktige kobling (totalt 8 poeng) og hvert kontekstbegrep (totalt 6 poeng).

KONTROLLPUNKT 4: FASIT – KOBLE BEGREPER

B 1. Retten til sletting	A 2. Rett til å reservere seg	E 3. Dataminimering	G 4. Kryptering
H 5. Datamegler	D 6. Samtykke	F 7. Nettfisking	C 8. Sporingsinformasjonskapsel

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 SAMTYKKE	2 DATAMEGLER	3 NETTFISKING	4 KRYPTERING
5 DATAMINIMERING	6 SLETTING		

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 B – FRAVALG	2 F – SAMTYKKE	3 E – DATAMEGLER	4 A – SLETTING
5 C – DATAMINIMERING	6 G – NETTFISKING	7 H – COOKIE	8 D – KRYPTERING

DISKUSJONSNOTATER TIL LÆRERE

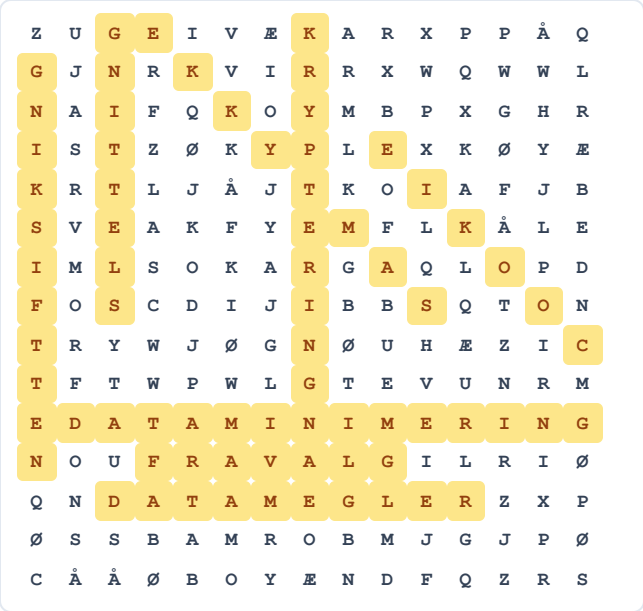
Nøkkelbegreper:
Kontroller at elevene kan forklare Retten til sletting, Rett til å reservere seg og Dataminimering med egne ord og gi et eksempel på hvert.

Casestudier:
Be elevene begrunne anbefalingene sine med fakta fra arbeidsarket i stedet for antakelser.

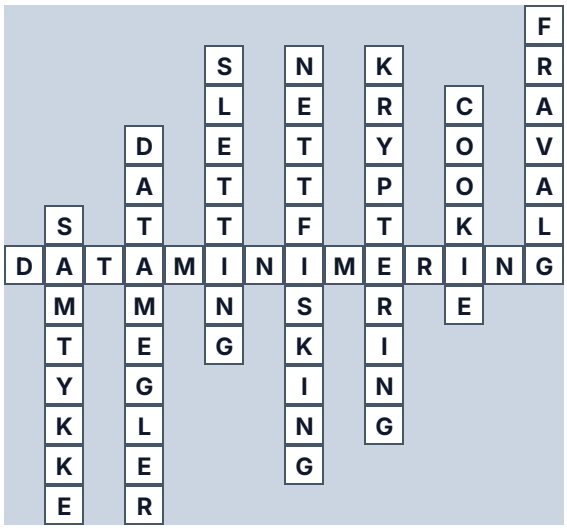
Kildevurdering:
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET



KRYSSORDLØSNING



LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

8 vannrett: DATAMINIMERING Prinsippet om å samle inn bare det som trengs for et angitt formål (14 bokstaver)

LODDRETT

1 loddrett: FRAVALG Rett etter CCPA til å stanse salg eller deling av dataene dine (7 bokstaver)

2 loddrett: SLETTING Rett som lar deg be en organisasjon slette personopplysningene dine (8 bokstaver)

3 loddrett: NETTFISKING Falske meldinger som lurer deg til å avsløre påloggінger eller kortopplysninger (11 bokstaver)

4 loddrett: KRYPTERING Å skramble data slik at bare den med riktig nøkkel kan lese dem (10 bokstaver)

5 loddrett: COOKIE Liten nettleserfil som kan følge aktiviteten din på tvers av nettsteder (6 bokstaver)

6 loddrett: DATAMEGLER Selskap som samler og selger profiler om personer (10 bokstaver)

7 loddrett: SAMTYKKE Fritt gitt, spesifikk, informert og utvetydig enighet om bruk av data (8 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

1. NTTSILGE — **SLETTING**
2. MAITNNDIIGERMA — **DATAMINIMERING**
3. DEEGAMRALT — **DATAMEGLER**
4. SNGITFIKNET — **NETTFISKING**
5. AGVAFLR — **FRAVALG**
6. NTPRIKREGY — **KRYPTERING**
7. SEYKKATM — **SAMTYKKE**
8. OECIKO — **COOKIE**

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"TENK FØR DU DELER PÅ NETT"

Fasit til casestudiene

A Casestudie 1: Be et nettsted om å slette data

Veiledning til læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: Maya, som bor i Frankrike, avsluttet kontoen sin i en handleapp for to år siden, men får fortsatt markedsførings-e-poster fra den. Hun vil at appen skal slette personopplysningene hennes i henhold til GDPR-retten til sletting.
- Anbefalte tilnærminger: Alternativ 1: Maya sender en skriftlig sletteforespørsel og protesterer mot direkte markedsføring, som da må stoppe; appen bør vanligvis svare innen én måned [1]. Alternativ 2: hun melder seg først av for rask lindring. Begrunnelse: sletting er ikke absolutt, så appen kan beholde data som trengs for juridiske forpliktelser eller rettskrav [1]. Hvis den ikke svarer, kan hun klage til personvernmyndigheten [1].

B Casestudie 2: En quiz-app og tillatelser

Veiledning til læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En gratis personlighetsquiz-app ber Leo om posisjon, kontakter, mikrofon og fødselsdato før han kan starte.
- Anbefalte tilnærminger: Alternativ 1: nekt tilgang til posisjon, kontakter og mikrofon, og sjekk deretter om quizen fortsatt fungerer [8]. Alternativ 2: hvis appen insisterer, velg en annen app eller slett den [8]. Begrunnelse: en quiz trenger sjelden disse dataene, og å dele mindre begrenser hva som kan samles inn, selges eller eksponeres. Leo kan også gjennomgå tillatelser regelmessig i telefonens personverninnstillinger [8].