

Alternativer til Big Tech – v. 8.6.25

Skrevet av Tech Mot Folkemord (techmotfolkemord.io)

Dette dokumentet inneholder anbefalinger til de mest kjente tjenestene og applikasjonene som mange bruker oftest i sin hverdag. Vi har laget listen med tanke på et bredt publikum, og foreslår alternativer som skal være lett å ta i bruk og/eller installere.

→ Vi har lagt vekt på alternativer som er fri og open-source så langt det lar seg gjøre.

→ Dokumentet, og nettsiden, er levende og oppdateres etterhvert som vi undersøker alternativer og sjekker personvern og sikkerhet.

Dersom du ønsker å foreslå alternativer vi bør ha med, eller du ønsker at vi skal finne alternativer til konkrete tjenester, så bruk vår anonyme tilbakemeldingsskjema:

<https://tally.so/r/wd4aQN>

Tabellen under er oppsummerende. Se påfølgende sider for mer detaljer.

Kategori	Anbefaling	Kommentar
Nettleser	Mac & iPhone, Safari uten reklame, sporing og identifisering: Safari + Proton VPN med NetShield	Safari sammen med Proton VPN gir sterkere sikring enn Chrome. Se punktene 1.1, 9 (Mac) og 10 (iPhone) for å sikre Safari. Best tilpasset Mac og iPhone, og sparer mye strøm.
	Beste løsning, alle plattformer: Vivaldi + Proton VPN med NetShield https://vivaldi.com (også tilgjengelig for mobiler)	Vivaldi er norsk-produsert nettleser. Den er reklamefri og sikker mot sporing. Bruk sammen med Proton VPN.
	Høy sikkerhet, men treg: Tor Browser (Mac & Android) + Proton VPN Onion Browser (iPhone) + Proton VPN	Dersom du ønsker å være 100% anonym og privat på nett, bruk Tor Browser eller Onion Browser sammen med Proton VPN.
Søkemotor	Startpage: https://www.startpage.com	Startpage er europeisk, og følger GDPR-regelverket. Henter resultater fra bla. Google.
	DuckDuckGo: https://duckduckgo.com	DuckDuckGo er sikker, men har et samarbeid med Microsoft.

Generativ AI	Duck.ai: https://duck.ai	Gir deg gratis, privat og anonym generativ ai. PS: Aldri skriv eller del personlig eller annen sensitiv informasjon!
E-post og Drive	Proton Mail og Proton Drive: https://proton.me/mail https://proton.me/drive	Pr. dags dato det sikreste som finnes. Proton Mail og Drive kan fåes gratis.
Kalender	Proton Calendar https://proton.me/calendar	Følger med som en del av Proton Mail.
Forms	Tally https://tally.so/	Belgisk produkt som følger GDPR-reglene. Mer detaljer i punkt 5 i detaljene nedenfor.
Docs (online)	CryptPad https://cryptpad.fr	Cryptpad er fransk selskap med sikkerhet i fokus.
	Proton Docs (en del av Proton Drive) https://proton.me/drive/docs	Proton Docs er et alternativ via sin Proton Drive-løsningen.
Docs (offline)	LibreOffice https://www.libreoffice.org	Alternativ til MS Office. Har innebygde alternativer til alle Office-produktene. Kan lagre filer som docx, pptx og xlsx.
Photos	Proton Albums (en del av Proton Drive) https://proton.me/drive/photo-storage	Fullt kryptert bilde-album.
Maps	WeGo https://wego.here.com/	WeGo er et fullt alternativ til Google Maps. Har live-info, kollektiv-info og ruteplanlegger.
	Magic Earth https://www.magicearth.com	Magic Earth er en navigasjonsapp for mobil/pad.
	Apple Maps Maps-appen i Mac og iPhone	Apple Maps er sikrere enn Google Maps. Deler svært lite data med tredje-parter.
Tegne-programmer	Draw.io (diagrammer) http://draw.io LibreOffice Draw (frihåndstegning)	Draw.io er et engelsk-sveitsisk selskap med sikkerhet i fokus.

Innhold

Anbefalinger og detaljert beskrivelse.....	4
1. Nettleser - Alternativer til Google Chrome og Microsoft Edge.....	4
1.1.1 Apple-maskiner (Mac & iOS).....	4
1.1.1 Windows-maskiner.....	4
1.2 Unngå Firefox:.....	5
1.3 Unngå Brave Browser og DuckDuckGo Browser.....	5
1.3.1 Brave.....	5
1.3.2 DuckDuckGo.....	5
1.4 Anbefaling - Tor Browser (Android & Mac), Onion Browser (iPhone).....	6
1.4.1 Tor Browser og Proton VPN (Macbook, Windows, Linux & Android).....	6
1.4.2 Onion Browser og Proton VPN (iPhone).....	7
1.5 Vår anbefaling (for alle operativ systemer, og mobiler):.....	7
2. Alternativ til Google Search.....	7
2.1 DuckDuckGo.....	7
2.2 Startpage.....	8
2.2 Vår anbefaling.....	8
3. Alternativer til ChatGPT, Claude, DeepSeek, Copilot.....	8
3.1 Anbefaling: Bruk AI-verktøy og AI-chat i privat modus.....	8
3.2 Vår anbefaling: Duck.ai.....	9
4. Alternativer til Google Gmail, Google Drive, Microsoft Outlook & OneDrive.....	9
4.1 Vår anbefaling: Proton Ultimate.....	9
5. Alternativ til Google Forms.....	10
5.1 Vår anbefaling: Tally.....	10
6. Alternativ til Google Photos – Proton Albums (en del av Proton Drive).....	10
7. Alternativ til Google Docs og Microsoft Office.....	10
7.1 Anbefaling: CryptPad (online).....	10
7.2 Anbefaling: Proton Docs (online).....	10
7.3 Anbefaling: LibreOffice (offline).....	10
8. Alternativ til Google Maps.....	11
8.1 Alternativ for iOS og Macbook - Apple Maps.....	11
8.2 Alternativ på nett - WeGo.....	11
8.3 Alternativ på mobil og pad – Magic Earth.....	12
9. Sikring av Safari - Macbook.....	12
10. Sikring av Safari – iPhone.....	13
11. Bytte standard søkemotor.....	14
11.1 Safari.....	14
11.2 Chrome.....	14
Kilder.....	15

Anbefalinger og detaljert beskrivelse

1. Nettleser - Alternativer til Google Chrome og Microsoft Edge

Google Chrome er en av verdens mest brukte nettlesere, men vi blir stadig mer oppmerksom på hvordan Google tilpasser sin nettleser til å samle mer og mer info om oss. Tilliten til Google og Microsoft er kraftig redusert på grunn av deres a) hensynsløse mål om å tjene mest mulig penger på våre private data via sporing, identifisering og reklame, og b) involvering og medskyld i folkemordet på palestinerne.

1.1.1 Apple-maskiner (Mac & iOS)

På veien til andre, sikrere nettlesere, kan et første steg være å bytte over til Safari fra Apple. På Macbooks og iPhones bruker Safari langt mindre strøm enn andre nettlesere, og kan derfor spare mye batteri og minne. Rett ut av boksen er ikke Safari den sikret, men med riktig innstillinger aktivert blir den mer privat, og forhindrer trackere fra å drive profilering og sporing på tvers av nettsider du besøker. Derfor er dette et godt første steg vekk fra Chrome/Chromium baserte nettlesere mens du vurderer andre nettlesere. Avansert blokkert av sporing og identifisering er kun aktivert for «private browsing» i Safari. Du må endre dette i innstillingene slik at all din aktivitet i Safari beskyttes.

1. Se skjermbildene i punkt 9 og 10 for å sikre Safari på Macbook og på iPhone.

2. Det er sterkt anbefalt å installere Proton VPN og aktivere funksjonen NetShield

 Med dette oppsettet har du god sikring mot sporing og identifisering på tvers av nettsider, men din nettaktivitet er fremdeles synlig innad i VPN-serverne.

 Sammen med ProtonVPN (med NetShield aktivert) blir du kvitt reklame, sporing (trackers) og skadelig programvare (malware) helt uten å installere farlige/ukjente plugins eller ad-blockere i Safari.

 Om du vil helt vekk Big Tech (også Safari), anbefaler vi å bytte til den norsk-produserte nettleseren Vivaldi og bruke dette sammen med Proton VPN med NetShield aktivert.

1.1.1 Windows-maskiner

 Microsoft Edge er en nettleser laget av Microsoft som kommer som standard med Windows-maskiner. Microsoft har de siste årene kraftig bygd opp sine reklame, annonserings- og sporings-kapabiliteter, og de er også skyldig og delaktig i folkemordet på palestinerne.

 Vi anbefaler sterkt å bytte til den norsk-produserte nettleseren Vivaldi, og bruke dette sammen med Proton VPN med NetShield aktivert.

1.2 Unngå Firefox:

Firefox var tidligere et alternativ kjent for å fokus på personvern, men vi anbefaler likevel ikke Firefox pr. dags dato. Grunnen til dette er at Mozilla, som lager Firefox, har ansatt tidligere produktsjef i Meta som ny Firefox produktleder (Ajit Varma). Det er flere utfordringer med dette, blant annet at Varma i sin tidligere jobb kommersialiserte WhatsApp. Vi vet også fra internasjonal etterforskning at WhatsApp data blir brukt i sporing og spionering av palestinere (kilde 1). Både ansettelsen av Varma, og Mozilla sin dreining mot kommersialisering av Firefox data er overraskende.

✗ Den viktigste grunnen til at vi ikke anbefaler Firefox, er at Mozilla ønsker å gjøre det enklere trekke ut data om sine brukere for å bygge sin ny AI-satning: Mozilla.ai. For å gjøre dette endret Mozilla sine "terms of usage" der endringen nå er at du gir Mozilla alle rettigheter til å bruke dine data (merk presiseringen til Mozilla: bruke dataene, ikke eie de). Mozilla har også fjernet alle slag som tidligere ble brukt i markedsføringen av Firefox om at de ikke solgte/brukte data om brukerne. Se kilde 2 og 3 for mer info.

✓ Ønsker du likevel å bruke en Firefox-variant, er Tor Browser et godt alternativ. Les mer om dette i punkt 1.4.

1.3 Unngå Brave Browser og DuckDuckGo Browser

1.3.1 Brave

Brave browser er et alternativ mange kjenner. Nettleseren fra Brave har god beskyttelse rett ut av boksen, men vi anbefaler ikke å bruke verken nettleseren eller søkemotoren fra Brave. Årsaken er Braves eier, Brendan Eich, som er kjent for å støtte anti-LGBTQ+ kampanjer. Eich er tidligere co-founder av Mozilla og mannen som fant opp JavaScript. Han fikk i 2014 sparken fra Mozilla på grunn av sin støtte til staten Californias lover som forbydde ekteskap mellom skeive par. Også i nyere tid har Eich opprettholdt sine anti-LGBTQ+ syn (kilde 4). Tech Mot Folkemord er allierte av alle skeive, og derfor er dette ikke en nettleser vi anbefaler.

✗ Unngå Brave

✓ Kjøp Amnesty International sin Regnbue-armbånd: <https://amnesty.no/regnbue>

1.3.2 DuckDuckGo

DuckDuckGo har vært en nettleser vi tidligere anbefalte, men som vi nå anbefaler å bruke med forsiktighet. Årsaken til dette er avsløringene om at DuckDuckGo samarbeider med Microsoft, og at nettleseren fra DuckDuckGo ikke blokkerte sporing knyttet til reklamer fra Microsoft, Bing, LinkedIn og andre Microsoft eide tjenester. DuckDuckGo har de siste to årene tatt grep og sier selv at de nå blokkerer sporing fra Microsoft. Bakgrunnen for samarbeidet med Microsoft er at søkeresultatene fra DuckDuckGo er fra Bing. Resultatene

rengjøres før det vises i DuckDuckGo -- men merk at bias i Microsoft Bing også vil synes i resultatene som vises i DuckDuckGo Search(mer info på kilder 6 og 7).

⚠ Ikke klikk reklamer. Vær oppmerksom på at du DuckDuckGo fremdeles kan tillate Microsoft å profilere brukere på nettsider de selv eier (som f.eks. LinkedIn, Bing, Github, Office, Outlook).

✅ Trygt å bruke søkemotoren fra DuckDuckGo, ingen tracking eller profilering (så lenge du ikke klikker på noe reklame).

1.4 Anbefaling - Tor Browser (Android & Mac), Onion Browser (iPhone)

Tor Browser er en open-source basert nettleser som er bygd på samme kildekode som Firefox. Tor, som er kort for «The Onion Router» er mest kjent for å være et nettverk som anonymiserer din lokasjon og nettaktivitet ved at all trafikk i nettleseren krypteres. Tor Browser kobler seg automatisk til Tor-nettverket når nettleseren startes.

All nettaktivitet inne i Tor Browser sendes gjennom et stort nettverk av noder over hele verden, noe som gjør det svært vanskelig å spore brukere. For verden ute, skjuler Tor både din fysiske lokasjon og nettsidene du besøker, mens din ISP/teleselskap kun ser at du kobler deg på Tor-nettverket (de kan ikke se hva du gjør i din nettleser mens den er inne i Tor-nettverket).

I land med høy sensur, har Tor vært avgjørende for at varslere, aktivister og menneskerettighetskjempere skal få tilgang til blokkerte eller sensurerte nettsider og tjenester. Edward Snowden brukte Tor-nettverket når han i 2013 avslørte NSA sin massive ulovlige overvåkning via PRISM-programmet.

Ønsker du søke nettet 100% anonymt og privat (ingen kan se din lokasjon), og uten å legge igjen spor etter deg, er Tor er det beste verktøyet du kan bruke.

Brukt alene er det flere risikoer Tor Browser. Nettleseren i seg selv blokkerer færre reklame og oppleves til tider svært tregt grunnet krypteringen av datatrafikken. Din lokasjon og nettaktivitet er også lett å avsløre for hackere og myndigheter inne i Tor-nettverket. Et annet kjent problem er at Tor-nettverket hyppig blir brukt til kriminalitet (f.eks. barnepornografi) og ulovlige DarkWeb sider (kriminelle nettsider). Tor-nettverket har de siste 5 årene også vært utsatt for flere hacker-angrep – **derfor er det helt essensielt å bruke Tor Browser sammen med en VPN-løsning – vår anbefaling er å bruke Proton VPN.**

1.4.1 Tor Browser og Proton VPN (Macbook, Windows, Linux & Android)

1. Først start Proton VPN, og koble til (enten med Quick Connect, eller en bestemt server, feks. Norge)
2. Last ned Tor Browser fra <https://www.torproject.org> og start nettleseren
3. I Tor Browser ser du først pålogging til Tor i skjermen «Connect to Tor». Klikk Connect.

4. Du skal nå være online i Tor-nettverket. Du kan verifisere dette ved å sjekke nettsiden <https://check.torproject.org/> og se at det står at du er riktig pålogget.

Dette oppsettet kalles «Tor over VPN» og er den sikreste måten å koble seg til Tor.

1.4.2 Onion Browser og Proton VPN (iPhone)

For iPhone må du bruke appen Onion Browser.

1. Først start Proton VPN på din iPhone, og koble til (enten med Quick Connect, eller en bestemt server, feks. Norge)

2. Gå til <https://onionbrowser.com> og last ned Onion Browser

3. Start Onion Browser og velg «Start built-in Tor»

4. Du skal nå være online i Tor-nettverket. Du kan verifisere dette ved å sjekke nettsiden <https://check.torproject.org/> og se at det står at du er riktig pålogget. (ps: du får varsel om at du ikke bruker «Tor Browser», dette kan du ignorere).

1.5 Vår anbefaling (for alle operativ systemer, og mobiler):

De aller færreste har behov for å være 100% anonym og usynlig på nettet. Vi anbefaler derfor ikke å bruke Tor-baserte nettlesere og Tor-nettverket som standard.

Vår anbefaling er å bruke den norske nettleseren Vivaldi sammen med Proton VPN. Den er basert på open-source koden til Chromium, men har sterk sikring mot uønsket profilering, sporing og reklame. Nettleseren fra Vivaldi er svært funksjonsrik, oppleves svært raskt og har god sikring rett ut av boksen (med andre ord trenger du ikke gjøre så mange endringer i innstillingene).

Det er sterkt anbefalt å bruke Proton VPN. Last ned her: <https://protonvpn.com>.

✓ Vivaldi - <https://vivaldi.com>

2. Alternativ til Google Search

2.1 DuckDuckGo

DuckDuckGo en søkemotor som er kjent for å hindre at du blir profilert basert på hva du søker. Dette er et kjent problem i Chrome, der alle søk du gjør lagres og brukes for å identifisere mest mulig informasjon om deg. Chrome rangerer også søkeresultatene etter hva de har profilert om deg og potensielle reklame-inntekter. Med DuckDuckGo profileres du ikke på tvers av nettsider når du gjør søk ettersom DuckDuckGo ikke lagrer eller logger dine søk. DuckDuckGo henter sine resultater fra Microsoft Bing.

Viktig: Fordi DuckDuckGo samarbeider med Microsoft, vil det tidvis vises reklame i søkeresultatene. Ikke klikk på reklamen, da enhver klikk på reklame vil gjøre at Microsoft kan spore og profilere deg.

2.2 Startpage

Startpage er en europeisk søkemotor utviklet i Nederland, i Haag. På samme måte som DuckDuckGo, forhindrer også Startpage at du spores og profileres basert på hva du søker. Et av det viktigste fordelene med Startpage er at det følger det europeiske GDPR-regelverket, og som følge av dette kan du i innstillingene velge å hente søkeresultater fra kun servere i EU. Startpage er standard søkemotor i den norske nettleseren Vivaldi.

En annen interessant funksjon i Startpage er såkalt «Anonymous View» som tillater deg å titte på nettsider fullstendig anonymt uten at nettsiden klarer å spore eller identifisere deg. Merk at ikke alle nettsider tillater dette, men våre tester viser det stort sett virker.

Merk: Startpage er ikke tilgjengelig i Safari, Chrome eller DuckDuckGo Browser.

<https://www.startpage.com>

2.2 Vår anbefaling

Dersom Startpage er tilgjengelig og du ønsker maksimal beskyttelse, bør du velge det grunnet deres sterkere etterfølgelse av GDPR-reglene.

DuckDuckGo er fremdeles en god søkemotor, så lenge du er varsom på hva du klikker av lenker som beskrevet over. Dersom Startpage ikke er tilgjengelig som alternativ, anbefaler vi DuckDuckGo.

Se punkt 11 for hvordan du bytter søkemotor i innstillingene.

3. Alternativer til ChatGPT, Claude, DeepSeek, Copilot

3.1 Anbefaling: Bruk AI-verktøy og AI-chat i privat modus

AI fra Google, OpenAI, Anthropic, Microsoft og DeepSeek ikke er sikre - alle dine prompts og søk brukes for å trene modellene.

Viktig: Merk at heller ikke Microsoft Copilot i nettleseren, som mange beskriver som det beste alternativet, er sikker. I dokumentet "[Terms of Use](#)" under punkt 5 står det tydelig at du gir Microsoft alle rettigheter til å bruke, endre og republisere hva som helst du gir av informasjon. Pass på!

Viktig: Enkelte AI-verktøy, slik som OpenAI / ChatGPT har et alternativ der du starte en ny chat i private-modus. Dette gjør at din input ikke huskes eller brukes til å trene ChatGPT. Det er viktig å understreke at dette på ingen måte er en garanti, så du anbefales å ikke skrive sensitive, private eller annen avslørende informasjon om deg.

3.2 Vår anbefaling: Duck.ai

Duck.ai er laget av DuckDuckGo. Denne nettsiden gir deg privat og anonymisert AI-chat, og du kan også velge ulike typer modeller du vil chatte med.

<https://duck.ai>

Viktig: Uansett hvilket AI-verktøy du bruker, så er det svært viktig at du ikke skriver eller deler personlig eller annen sensitiv informasjon!

4. Alternativer til Google Gmail, Google Drive, Microsoft Outlook & OneDrive

Produktene fra Google og Microsoft er gratis, men alt som er gratis har likevel en kostnad. Google og Microsoft analyserer og profitterer på all data, også fra våre innboks, drive og docs. Vi anbefaler å redusere bruken av disse tjenestene, og å være svært selektiv med hva du bruker dem til.

4.1 Vår anbefaling: Proton Ultimate

I øyeblikket er sveitsiske selskapet Proton og de ulike Proton-produktene et av de sikreste alternativene som finnes. Det er laget av forskere i CERN (i Geneva), er open-source og har et særdeles sterkt fokus på kryptering og personvern. Dette gjør Proton Mail og Proton Drive til to særdeles gode alternativer til produkter fra Big Tech.

Viktig: Proton og alle dens produkter er open-source, og de finnes i gratis-versjoner. Vi anbefaler dog å investere i Proton Ultimate som gir deg tilgang til alle Protons produkter uten begrensning.

Viktig: Å bytte over krever å endre alle tjenester og adresser over til Proton, dette tar tid, men det er verdt det. E-post er av de absolutt mest sensitive tingene vi har, og en plass mange oppbevarer mye viktig info. Derfor er det meget viktig å bytte over til et alternativ som ikke spionerer på dine data.

<https://proton.me>

5. Alternativ til Google Forms

5.1 Vår anbefaling: Tally

Tally er belgisk og følger de europeiske data- og persnverns direktivene (GDPR), se kilde 5. Tally er et meget kraftig og gratis verktøy som gir deg avanserte forms og tilpasningsmuligheter. Tally gratis og har mange plugins og integrasjonsmuligheter. Oppgraderer du til en betalt versjon får du mulighet til å integrere Tally med ditt eget domene og mye mer. Se <http://tally.so/>

6. Alternativ til Google Photos – Proton Albums (en del av Proton Drive)

Proton Albums er bygd inn i Proton Drive og er et kryptert alternativ til Google Photos og andre.

7. Alternativ til Google Docs og Microsoft Office

7.1 Anbefaling: CryptPad (online)

CryptPad er en gratis online tjeneste med en svært bred produkt-katalog, der alt innhold krypteres. Det er fullstendig open-source og har en god gratis-versjon. CryptPad utvikles i Frankrike av et open-source selskap i Paris. All data hostes på franske servere.

<https://cryptpad.fr>

7.2 Anbefaling: Proton Docs (online)

Proton har et produkt som heter Proton Docs, som du får tilgang til via Proton Drive. Dokumentene dine blir kryptert og heller ikke Proton selv har tilgang til innholdet. Proton sine produkter finnes i både gratis- og betal-versjoner med mer plass.

<https://proton.me/drive>

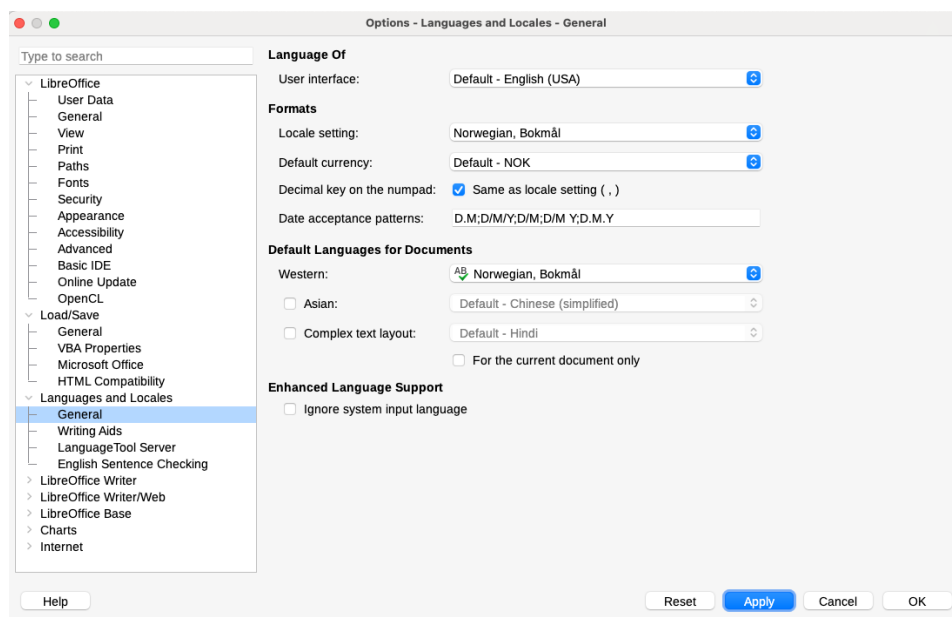
7.3 Anbefaling: LibreOffice (offline)

LibreOffice er open-souce og et helt gratis alternativ til Microsoft Office. LibreOffice har svært gode alternativer til alle Office-produktene: Writer (alternativ til Word), Spreadsheet (alternativ til Excel), Impress (alternativ til PowerPoint). Den har også et tegneprogram kalt Draw. LibreOffice produktene er fullt kompatibelt med Microsoft Office.

<https://www.libreoffice.org>

Viktig: Dersom du ønsker full kompatibilitet med Microsoft Office, husk å lagre dokumentene i riktig format:

- ▶ Writer (Word): File → Save (nye dokumenter) / Save As (for å lage kopi) → I feltet “File type” velger du “*Word 2010-365 Document (.docx)*”
- ▶ Spreadsheet (Excel): Samme som over, men velg “*Excel 2007-365 (.xlsx)*”
- ▶ Impress (PowerPoint): Samme som over, men velg “*PowerPoint 2007-365 (.pptx)*”



Figur 1: Tips: Husk å sette standardspråket i LibreOffice til norsk i innstillingene

8. Alternativ til Google Maps

Det finnes få alternativer til Google Maps som er gratis med tilsvarende funksjonalitet. Her er noen alternativer.

8.1 Alternativ for iOS og Macbook - Apple Maps

Apple Maps er en innebygd app i iOS og Macbook. Applikasjonen følger de samme personvern-reglene for Apple's øvrige produkter.

8.2 Alternativ på nett - WeGo

Veldig bra live info om trafikk og kollektivt, og bra ruteplanlegging (også via nettleser på laptop). De følger GDPR-regelverket og selger ikke data om brukerne i følge privacy-policyen.

<https://wego.here.com/>

8.3 Alternativ på mobil og pad – Magic Earth

Gratis og funksjonsrik navigasjonsapp for mobil. Bruker OpenStreetMap i bunn, og data som sendes ut anonymiseres med en skiftende nøkkel (endrer seg hvert 5 minutt).

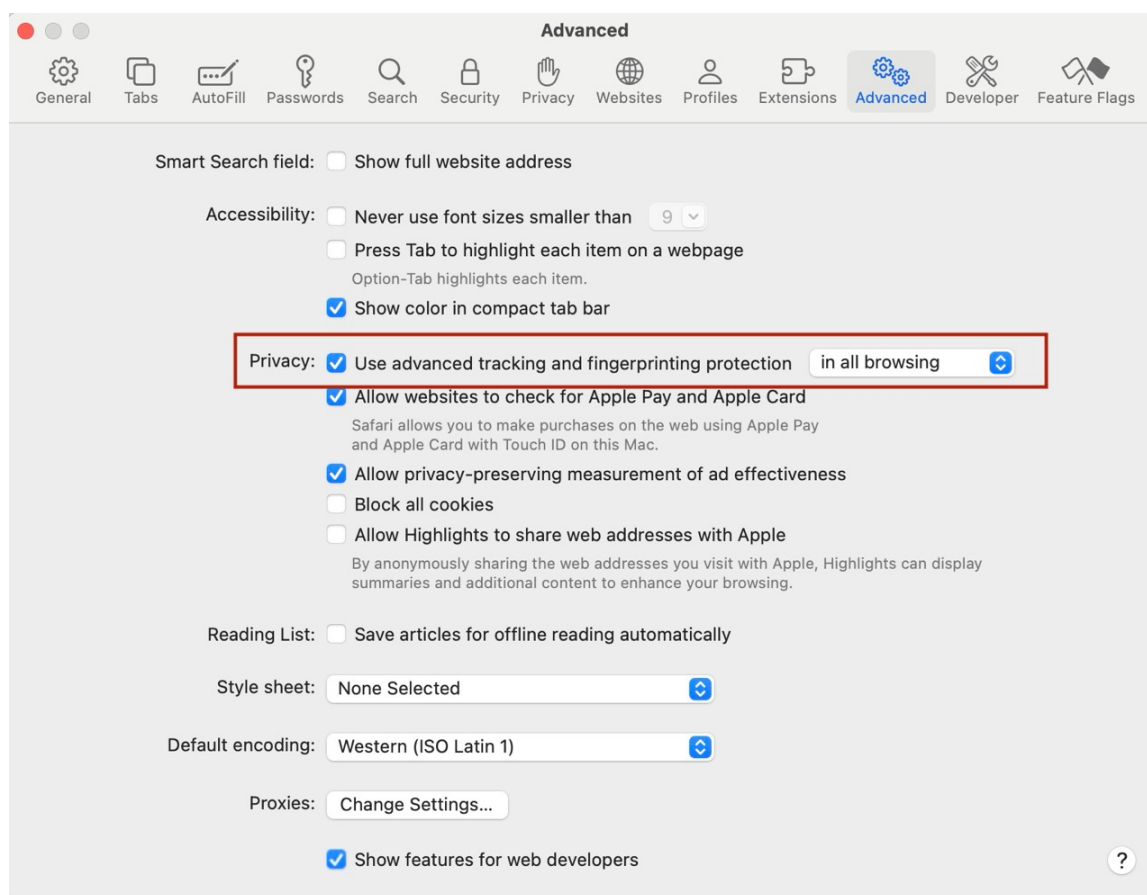
Privacy-policyen sier at de ikke samler eller selger data om brukere.

<https://www.magicearth.com>

9. Sikring av Safari - Macbook

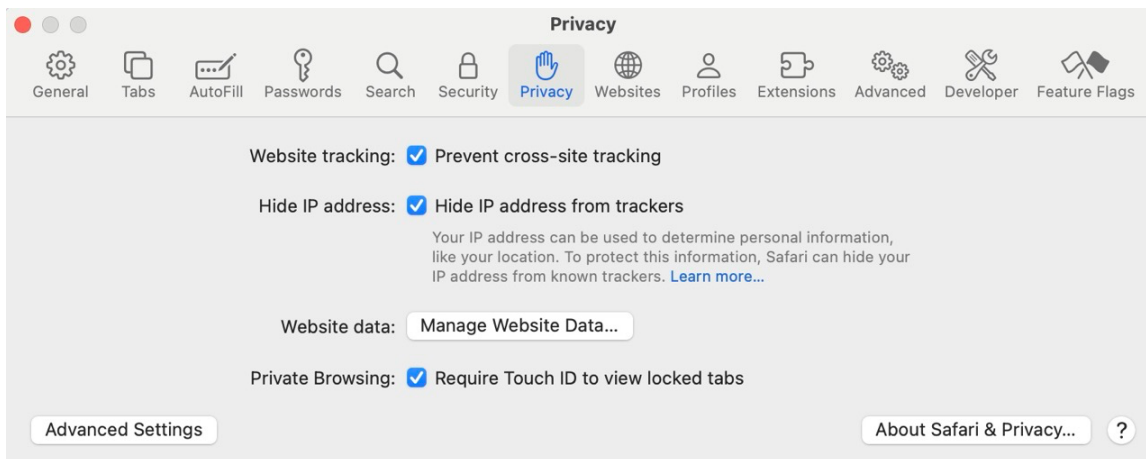
9.1) Pass på at beskyttelse mot tracking og fingerprinting er aktivert:

Velg «in all browsing» i feltet «Use advanced tracking and fingerprinting protection».



9.2) Pass også på at skjuling av IP og cross-site tracking er aktivert:

Velg «Hide IP-address from trackers» og «Prevent cross-site tracking».



10. Sikring av Safari – iPhone

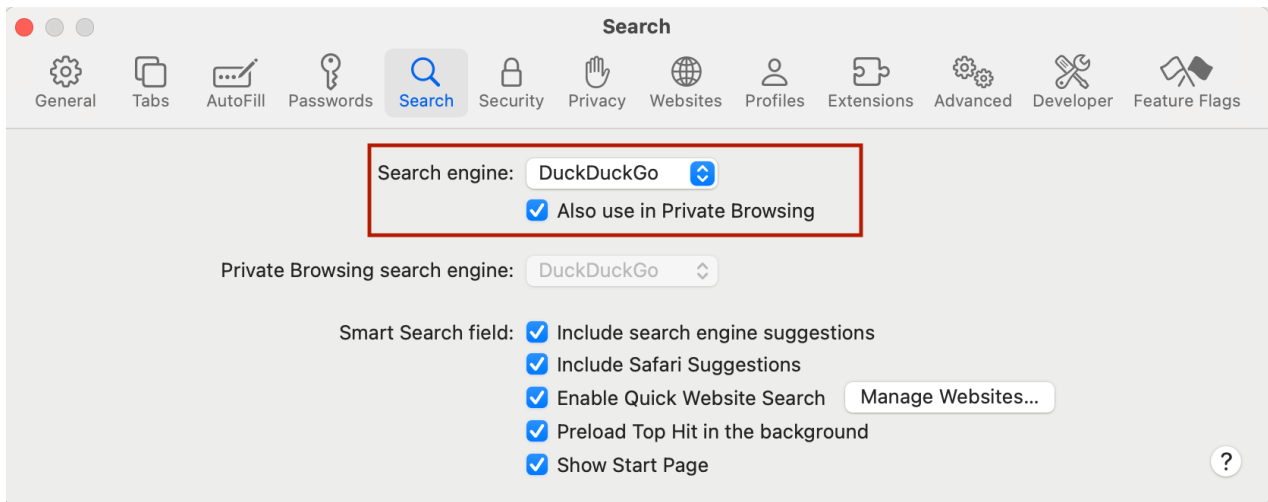
1. Gå til Settings
2. Skroll ned til Apps og deretter klikk på Safari
3. Sjekk at innstillingen "Prevent Cross-Site Tracking" er aktivert
4. Sjekk at innstillingen "Fraudulent Website Warning" er aktivert
5. Sjekk at innstillingen "Not Secure Connection Warning" er aktivert
6. Skroll videre helt ned til Advanced / Avansert
7. Klikk på Advanced Tracking and Fingerprinting Protection
8. Velg All Browsing

PS: Med jevne mellom, slett innholdet også i "Website Data" mappen.

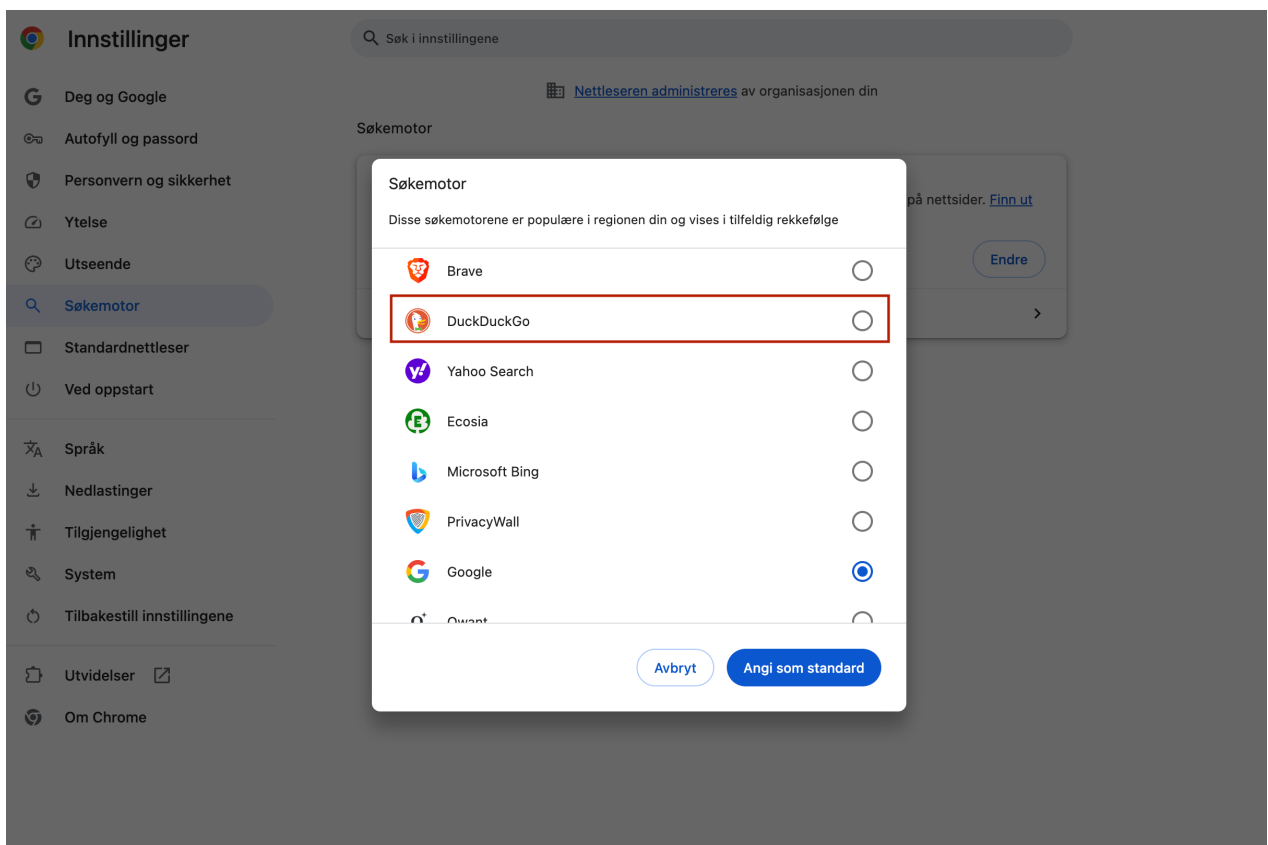
PS: Dersom Apple Intelligence er aktivert: Klikk på "Apple Intelligence" og deretter skru av "Learn from this App".

11. Bytte standard søkemotor

11.1 Safari



11.2 Chrome



Kilder

- 1 - <https://www.middleeastmonitor.com/20240418-israel-using-metas-whatsapp-to-kill-palestinians-in-gaza-through-ai-system/>
- 2 - <https://www.zdnet.com/article/the-firefox-i-loved-is-gone-how-to-protect-your-privacy-on-it-now/>
- 3 - <https://www.kode24.no/artikkel/raser-etter-at-mozilla-ikke-lenger-lover-a-ikke-selge-brukerdata/82765550>
- 4 - <https://community.brave.com/t/brave-needs-to-address-brendan-eich/281044>
- 5 - <https://tally.so/help/gdpr>
- 6 - <https://www.tomsguide.com/news/duckduckgo-privacy-browser-facing-backlash-over-microsoft-trackers>
- 7 - <https://www.cnet.com/tech/services-and-software/duckduckgo-will-block-more-microsoft-tracking-scripts/>