GDPR Sjekkliste

WordPress og WooCommerce

Skrevet av:

André Giæver

Senior Rådgiver for netthandel

Human Web

Innholdsfortegnelse

Introduksjon 2

Steg 1: WooCommerce Vilkår & Betingelser (VB) 4

Steg 2: WooCommerce Personvern 5

Steg 3: WooCommerce Brukerregistrering 6

Steg 4: WooCommerce - Forlatt handlekurv 7

Steg 5: WooCommerce kundeomtaler 8

Steg 6: WordPress kommentarer 9

Steg 7: WordPress og WooCommerce Opt-in skjemaer 10

Steg 8: WordPress kontaktskjemaer 11

Steg 9: WooCommerce Analytics 12

Steg 10: WordPress og WooCommerce Plugins 13

Steg 11: WordPress og WooCommerce API-er 14

Steg 12: Opplysningsplikt ved datalekkasje 15

Steg 13: Samtykke fra eksisterende brukere 16

En kort oppsummering 17

Alle To-do lister samlet 18

Introduksjon

Det florerer av GDPR-relatert innhold på nettet for tiden. Ingen vet ennå hva det nye reglementet for personvern vil innebære i praksis. Ingen vet hvor hardt det vil bli håndhevet i starten heller. Det vi vet er at fra ~~25. mai~~ 1. juli i år vil reglene tre i kraft. På tide å få hodet opp av sanden altså!

Dette er kortfattet hva vi foreløpig vet:

- Gjelder all virksomhet som behandler data på vegne av **personer innenfor EU**
- Krav til total transparens i forhold til **hvilke brukerdata** en virksomhet besitter
- Krav til **aktiv samtykke** før innsamling av data
- Krav til full **sletting** av brukerdata ved forespørsel fra bruker
- Virksomheter **kan bøtelegges** inntil 20 millioner Euro eller 4% av virksomhetens totale omsetning

Som nettbutikkeier eller eier av en nettside med registrering og behandling av brukerdata er du å regne som en **databehandler** og derfor underlagt GDPR. Jeg har skrevet denne artikkelen som stegvis sjekkliste for hva du som databehandler kan og bør gjøre.

> Dersom du trenger hjelp til å gjøre nettbutikken/nettsiden **GDPR-compliant** kan Human Web bistå med dette.

I verdenen av WordPress og WooCommerce er det **mange hensyn** å ta i forhold til datainnsamling. Mange ulike deler av systemet samler data. Du står ansvarlig for alle **3. parts integrasjoner** du bruker og er følgelig ansvarlig for at også disse er GDPR-compliant. Så bruker du systemer for å tracke og håndtere brukerdata?

Er svaret ja, bør du absolutt lese videre!

Steg 1

WooCommerce Vilkår & Betingelser (VB)

En egen side for VB er noe alle nettbutikker er påkrevd å ha. Dette er ingenting nytt ettersom det allerede er et **norsk lovkrav**, men det er også et krav under GDPR.

I **WooCommerce** må du først opprette en side for VB. Deretter må du legge til denne siden under *WooCommerce → Instillinger → Kasseinnstillinger*. Når dette er gjort vil du se at en **avkrysningsboks for samtykke** av VB dukke opp på kassesiden for nettbutikken.

Det er verdt å nevne at selv om du ikke selger varer eller tjenester direkte via en nettbutikk så bør en side for VB være tilgjengelig på nettsiden din. Det vil også bli et krav til aktiv samtykke (signering eller annen bekreftelse) på at det er lest før kjøp gjennomføres.

To-do liste:

- **Opprett** en side for vilkår og betingelser
- Hvis du allerede har en slik side, legg til en **GDPR-paragraf** som linker til siden din for Personvern (vi kommer tilbake til denne siden nedenfor)
- **Legg til** Vilkår og betingelser i WooCommerce

Steg 2

WooCommerce Personvern

Det er her, under behandling av personvern, GDPR har sitt treffpunkt. Du har krav på å informere brukeren om hvilke data du samler inn, hvordan de lagres og brukes.

Personvernteksten må dekke følgende:

- **Hvem du er** (firma, adresse, etc.)
- **Hvilke data** du samler inn (IP-adresser, navn, epost, telefon, adresse, etc.)
- **Årsaken** til at du samler dataene (fakturering, tracking, epost-kommunikasjon, etc.)
- **Hvilke 3. parter** som mottar data fra deg (MailChimp, CRM, Regnskap, etc.)
- **Hvordan dataene** kan lastes ned (automatisk eller ved kontakt med deg)
- **Hvordan dataene** kan slettes (automatisk eller ved kontakt med deg)
- **Hvordan komme i kontakt** med deg for data-relaterte spørsmål. (eller til personen som er ansvarlig for dette i din bedrift)

Merk! WordPress jobber i disse dager med en **Personverngenerator** som sannsynligvis vil legges under *Verktøy* i WotdPress Dashboard..

Nå som du har skrevet teksten må du vise en **link til Personvern** på alle sider av nettbutikken/nettsiden din. Dette gjør du enkelt ved å legge linken i footeren. I tillegg må du legge til en avkrysningsboks for **alle ulike skjemaer** du har på siden din. Dette gjelder brukerregistrering, epostskjema, nyhetsbrev, etc. Dette betyr at du må legge til en ekstra avkrysningsboks **på kassesiden også**.

> Vi har laget en liten **kodesnutt for en avkrysningsboks** på kode.humanweb.no. Registrer deg med et basis medlemskap, det er gratis første måneden.

Merk! avkrysningsboksene kan **ikke være krysset av** på forhånd. Brukeren må aktivt krysse av for at det skal anses som en **gyldig samtykke**.

To-do liste:

- **Opprett** en side for Personvern dersom du ikke har en allerede, ev. vent til WordPress er klar med sin generator
- **Legg til** hvem-hva-hvordan-hvorfor-når i Personvernerklæringen
- **Vis link** til Personvern i footer
- **Legg til** avkrysningsboks for Personvern på kassesiden

Steg 3

WooCommerce Brukerregistrering

Hvis du bruker WooCommerce og har **åpnet for registrering av brukere** via *Min konto* vil den ha et registreringsskjema med brukernavn og passord. (du aktiverer dette under *WooCommerce > Innstillinger > Kontoer > Aktiver kunderegistrering på "Min konto"-siden*)

Ettersom brukernavn og passord regnes som personlige data, **må vi legge til en avkrysningsboks** for personvern ved registrering, likt den på kassesiden,

> Vi har laget en liten **kodesnutt for en avkrysningsboks** på kode.humanweb.no. Registrer deg med et basis medlemskap, det er gratis første måneden.

Merk! Ved registrering, etterspør kun de brukerdata som du trenger for å drive virksomheten din. Vi kommer nærmere inn på dette senere.

To-do liste:

- Sjekk om du har aktivert for brukerregistrering i WooCommerce
- Hvis ja, legg til avkrysningsboks for Personvern i registreringsskjema

Steg 4

WooCommerce - Forlatt handlekurv

Forlatt handlekurv (abandoned cart) er en funksjon som **rammes hard** av GDPR. Plugins som gir deg denne funksjonaliteten samler inn **epostadresser uten samtykke**.

Dette går helt imot de nye reglene som krever en aktiv handling, dvs. at brukeren krysser av for å samtykke. Inntil videre er dette en funksjonalitet som **ikke støttes** av GDPR.

Forhåpentligvis vil plugin-forfattere som levere denne funksjonen finne smidige måter å hente inn samtykke fra brukeren.

Du har i realiteten to valg:

1. Kasseside i flere steg der du hindrer brukeren å gå videre til neste steg før kunden samtykker til at du samler inn epostadressen. Et veldig dårlig alternativ ettersom kassesider i flere steg konverterer veldig dårlig.

2. Deaktivere gjestekasse i nettbutikken. Dette er heller ikke noe godt alternativ, men på denne måten må brukeren opprette en konto for å kunne gå til kassen. Dårlig for konvertering, bra for GDPR.

To-do liste:

- **Kontakt utviklerne** av plugins med denne funksjonen og krev at de finner en løsning

Steg 5

WooCommerce kundeomtaler

Kundeomtaler er viktige, ikke sant? Utfordringen er at de **inneholder personlige data** og således krever samtykke.

En fin måte å håndtere utfordringen på er kun å tillate kundeomtaler fra **kunder som har kjøpt produktet** (*under WooCommerce > Innstillinger > Produkter > Generelt > Kundeomtaler kan kun lages av "bekreftede eiere").*

Ja, det er et lite, men **akseptabelt kompromiss** ettersom du allerede har fått samtykke fra kunden når produktet ble kjøpt.

To-do liste:

- **Kryss av** for *Kundeomtaler kan kun lages av "bekreftede eiere* i WooCommerce-instillingene

Steg 6

WordPress kommentarer

Hvis du tillater kommentarer på innlegg eller sider vil dette omfattes av GDPR.

Normalt sett vil brukere bli spurt om navn, epost og nettside sammen med sin kommentar uten krav om å opprette konto. **Dersom du allerede har implement steg 3** i denne sjekklisten og krever innlogging for å legge igjen kommentar, er du allerede i tråd med reglene.

Informasjonen som samles inn ved at en bruker legger inn en kommentar inkluderer både IP-adresse og cookies for at WordPress skal kunne "huske" brukere til senere. I tillegg lagres informasjonen under *Kommentarer* i WordPress Dashboard, samt en rekke andre steder.

Igjen er **løsningen relativt enkel** ved at du legger til en avkrysningsboks ved registreringen av kommentaren slik at du får hentet inn samtykket du trenger.

To-do liste:

- **Benytt** standard WordPress kommentarskjema (WordPress vil gjøre dette GDPR-compliant snart) eller bruk en kommentar-plugin der dette allerede er implementert.

Steg 7

WordPress og WooCommerce Opt-in skjemaer

Et opt-in skjema er et **registreringsskjema** der brukeren legger inn sitt navn og epostadresse (normalt sett) for å bli med på din epostliste, nyhetsbrev, etc.

Det første du må gjøre er å **fjerne alle automatiske opt-ins** på nettstedet ditt. Ingen av avkrysningsboksene kan være markert fra før av ettersom dette ikke er aktiv samtykke og derfor ikke gyldig aksept.

I alle tilfeller må du:

- **innhente** samtykke
- **forklare** hvorfor deres data trengs (eks: "legg inn eposten din for å motta ukentlig nyhetsbrev")
- **etterspørre** kun relevant informasjon (for nyhetsbrev trengs ikke fødselsdato, med mindre du vil sende de en gave på denne dagen. I så fall må du fortelle dette. Dessverre, ingen overraskelser...)
- **informere** om hvordan å slette/laste ned dataene når brukeren ønsker
- vise hvordan man melder seg ut

Merk! Uansett hvem du sender brukeren epostadresse til, sørg for at de er pålitelig og at de aktivt jobber for å bli GDPR-compliant.

To-do liste:

- **Gå gjennom** alle opt-in skjemaene på nettstedet ditt
- **Sjekk** om de som leverer opt-in skjemaene dine har en GDPR-løsning
- **Sørg for** å ha en obligatorisk avkrysningsboks for Personvern i alle skjemaene

Steg 8

WordPress kontaktskjemaer

I WordPress får vi gjerne kontaktskjemaer via plugins som Contact Form 7, Gravity Forms eller vår personlige favoritt, WPForms. Enten du benytter Google Analytic eller tilsvarende **samler du inn brukerdata uten samtykke via cookies**. Samme gjelder for Google Adwords, Facebook piksler og lignende.

Disse skjemaene krever nå samtykke for personvern.

Legg derfor til en avkrysningsboks, gjerne rett over "Send"-knappen for å innhente samtykke.

To-do liste:

- **Legg til** en avkrysningsboks i alle kontaktskjemaer
- Hvis skjemaene dine samler inn data for lagring, det gjør (nesten) alle, og **forklare nøyaktig** hvorfor du trenger dataene og hvor de lagres

Steg 9

WooCommerce Analytics

Datainnsamling og analyse av data er en viktig del for å forstå hva som skjer og hvordan man kan forbedre seg. Google Analytics er nok det mest utbredte verktøyet i denne sammenheng, men **alle slike verktøy samler og behandler data**.

Det beste er å sjekke med hvert enkelt verktøy sin GDPR policy, fordi **det er de som samler inn dataene, ikke du**. Du er altså ikke databehandler i denne sammenheng, men en **dataansvarlig**. Det er altså ditt ansvar, på vegne av brukerens data, å finne en databehandler som er GDPR-compliant. **Ser du forskjellen?**

I følge Google Analytics Teamet (de sendte ut en epost til alle kontoansvarlige 11.april 2018):

- GDPR krever din oppmerksomhet og handling, selv om dine brukere ikke holder til i European Economic Area (EEA)
- Vi har introdusert granulær datalagringskontroll som lar deg velge hvor lenge dine bruker- og hendelsesdata lagres på våre servere. Google analytics vil automatisk slette bruker- og hendelsesdata som er eldre en varigheten du har satt
- Før 25. mai vil Google Analytics også introdusere et verktøy for å slette brukere ved å la deg slette alle data assosiert til en enkel bruker (en besøkende) fra dine områder i Google Analytics
- GA vil fortsette å levere tjenester som skreddersydde innstillinger for cookies, personvernkontroll, instillinger for deling av data, sletting av data ved avslutting av konto og annonymisering av IP.

To-do liste:

- **Benytt kun** pålitelig og GDPR-compliant tracking-verktøy
- **Spør leverandørene** av software hva de gjør for å være i samsvar med GDPR
- **Legg til** i Personvernerklæringen din hvem som behandler data på dine vegne.

Steg 10

WordPress og WooCommerce Plugins

Dette er **et veldig viktig steg**, men jeg vil forsøke å oppsummere det raskt. Følg denne malen for samtlige plugins du bruker på alle nettsteder du administrerer:

Gør pluginen noe av det følgende; henter, leser, lagrer, bruker, redigerer eller håndterer har tilgang til personlige data?

Hvis svaret er ja:

- sørg for at det er pluginen og dens utviklere er pålitelige
- sørg for at de jobber for å gjøre pluginen GDPR-compliant
- sørg for å legge pluginen til under 3. parts leverandører i personvernerklæringen

Hvis svaret er nei:

- er du sikker?
- er du helt sikker?
- Ok, så bra. Da trenger du ikke gjøre noe

To-do liste:

- **Gå gjennom** alle plugins
- **Legg til** plugins som berører GDPR i personvernerklæringen

Steg 11

WordPress og WooCommerce API-er

API-er er noe de færreste av oss ligger å drømmer om om natten, så la meg først forklare hva et API er. Et **API (Application Programming Interface)** er kort sagt en "bolk med kode" som lar deg kommunisere med et ekstern system sin software uten at du trenger å forlate ditt eget.

API-er brukes til å **flytte data mellom to parter**. En god analogi vil være å tenke på en ekstremt kjedelig dialog på epost mellom to mennesker (de spør og svarer på de samme spørsmålene hele tiden). Menneskene er API-ene og dataene de sender er epostene med informasjon. Hvis disse spørsmålene eller svarene inneholder personlig informasjon så gjelder GDPR for denne dialogen.

Eksempler:

- brukere kan melde seg på din MailChimp liste uten selv å være i kontakt med MailChimp
- brukere kan bruke Stripe som betalingsløsning i nettbutikken din uten å kontakte Stripe

Facebook, Twitter og andre former for 3. parts software har også API-er. Disse API-ene **knytter WooCommerce til verden utenfor** ved å sende - muligens personlig og privat brukerdata.

Det som er viktig for deg å vite, er følgende:

- hvilke API-er du bruker
- hva slags data som sendes
- om API-et er GDPR-compliant

Har du dette i orden er du på trygg grunn. API-ene du bruker **skal listes i personvernerklæringen** med forklaring på hva hvert enkelt håndterer av brukerdata.

Todo liste:

- **Gå gjennom** alle API-ene du bruker
- **Kutt ut** API-er som ikke er GDPR-compliant
- **Legg til** liste over API-er i personvernerklæringen

Steg 12

Opplysningsplikt ved datalekkasje

Som del av GDPR har du opplysningsplikt dersom nettstedet ditt er utsatt for en datalekkasje. Du skal informere berørte brukere **innen 72 timer**.

- Hva er datalekkasje, tenker du kanskje?

Dette vil gjelde hvis personlig informasjon er sendt til:

- en kilde som ikke brukeren har samtykket til
- en instans som ikke er GDPR-compliant
- en 3. part uten at bruker vet om det
- en hacker

I tillegg til dette må du kunne **fremvise en plan** for hvordan virksomheten din vil håndtere en eventuell datalekkasje.

To-do liste:

- **Sørg for** at WordPress/WooCommerce nettstedet ditt er sikkert og oppdatert
- **Abonnér** på alle nyhetsbrev, statusmeldinger, etc. fra dine 3. parts tjenester /API-leverandører slik at du får vite om eventuelle datalekkasjer hos dem som påvirker deg og dine brukere
- **Redusere** datamengden du lagrer.
- **Ha en kriseplan** klar for eventuell datalekkasje

Steg 13

Samtykke fra eksisterende brukere

Sjansene er store for at du allerede har mottatt flere forespørsler fra nettjenester, apper, etc. om at de nylig har oppdatert Vilkår og betingelser, samt sin personvernerklæring. **Alle disse krever** at du aktivt samtykker til disse oppdateringene.

Dette er fordi **GDPR er retroaktivt**. Det gjelder altså tidligere registrerte brukere og deres personlige lagrede brukerdata.

Som du sikkert nå forstår så må også du **kontakte dine eksisterende brukere** for aktivt å fornye samtykke. Du må samtidig **opplyse dem om hvor og hvordan** de kan få tilgang til og mulighet til å laste ned eller slette sine brukerdata.

Likevel kan det tolkes litt fritt **dersom samtykket som tidligere** har blitt gitt allerede har fulgt GDPR sine retningslinjer.

To-do liste:

- **Kontakt eksisterende** kunder for aktivt samtykke av oppdatert Vilkår og betingelser, samt personvernerklæring

En kort oppsummering

Vi kan være sikre på at GDPR kommer og at det kommer til å ha stor effekt på de av oss som behandler data på vegne av brukere. Men i mine øyne er GDPR en **positiv** ting som vi alle bør sette pris på som brukere av internett.

Vi kan nok være tilsvarende sikre på at **verden ikke kommer til å gå under** eller forandres urovekkende mye. Med unntak av noen statuerende eksempler fra myndighets hold vil nok de fleste kunne ta det med ro. Dette er en enorm implementering og den **vil ta mange år**.

Det viktigste er at du er "i prosess", og med denne sjekklisten har du forhåpentligvis fått en stjerne å følge. Du er naturligvis hjertelig velkommen til en prat med oss i Human Web dersom du trenger litt støtte på veien.

Lykke til!

André Giæver

Senior Rådgiver for ehandel

Human Web

Alle To-do lister samlet

Steg 1: WooCommerce Vilkår & Betingelser (VB)

- **Opprett** en side for vilkår og betingelser
- Hvis du allerede har en slik side, legg til en **GDPR-paragraf** som linker til siden din for Personvern (vi kommer tilbake til denne siden nedenfor)
- **Legg til** Vilkår og betingelser i WooCommerce

Steg 2: WooCommerce Personvern

- **Opprett** en side for Personvern dersom du ikke har en allerede, ev. vent til WordPress er klar med sin generator
- **Legg til** hvem-hva-hvordan-hvorfor-når i Personvernerklæringen
- **Vis link** til Personvern i footer
- **Legg til** avkrysningsboks for Personvern på kassesiden

Steg 3: WooCommerce Brukerregistrering

- Sjekk om du har aktivert for brukerregistrering i WooCommerce
- Hvis ja, legg til avkrysningsboks for Personvern i registreringsskjema

Steg 4: WooCommerce - Forlatt handlekurv

- **Kontakt utviklerne** av plugins med denne funksjonen og krev at de finner en løsning

Steg 5: WooCommerce kundeomtaler

- **Kryss av** for *Kundeomtaler kan kun lages av "bekreftede eiere* i WooCommerce-instillingene

Steg 6: WordPress kommentarer

- **Benytt** standard WordPress kommentarskjema (WordPress vil gjøre dette GDPR-compliant snart) eller bruk en kommentar-plugin der dette allerede er implementert.

Steg 7: WordPress og WooCommerce Opt-in skjemaer

- **Gå gjennom** alle opt-in skjemaene på nettstedet ditt
- **Sjekk** om de som leverer opt-in skjemaene dine har en GDPR-løsning
- **Sørg for** å ha en obligatorisk avkrysningsboks for Personvern i alle skjemaene

Steg 8: WordPress kontaktskjemaer

- **Legg til** en avkrysningsboks i alle kontaktskjemaer
- Hvis skjemaene dine samler inn data for lagring, det gjør (nesten) alle, og **forklare nøyaktig** hvorfor du trenger dataene og hvor de lagres

Steg 9: WooCommerce Analytics

- Benytt kun pålitelig og GDPR-compliant tracking-verktøy
- Spør leverandørene av software hva de gjør for å være i samsvar med GDPR
- Legg til i Personvernerklæringen din hvem som behandler data på dine vegne.

Steg 10: WordPress og WooCommerce Plugins

- Gå gjennom alle plugins
- Legg til plugins som berører GDPR i personvernerklæringen

Steg 11. WordPress og WooCommerce API-er

- Gå gjennom alle API-ene du bruker
- Kutt ut API-er som ikke er GDPR-compliant
- Legg til liste over API-er i personvernerklæringen

Steg 12: Opplysningsplikt ved datalekkasje

- Sørg for at WordPress/WooCommerce nettstedet ditt er sikkert og oppdatert
- Abonnér på alle nyhetsbrev, statusmeldinger, etc. fra dine 3. parts tjenester /API-leverandører slik at du får vite om eventuelle datalekkasjer hos dem som påvirker deg og dine brukere
- Redusere datamengden du lagrer.
- Ha en kriseplan klar for eventuell datalekkasje

Steg 13: Samtykke fra eksisterende brukere

- Kontakt eksisterende kunder for aktivt samtykke av oppdatert Vilkår og betingelser, samt personvernerklæring