ubivox guide

GDPR og nyhedsbreve

Sådan undgår du faldgruberne i din e-mailindsats

Er GDPR-reglerne ikke bare sat i verden for at gøre mit arbejde sværere?

Det kan man hurtigt tage sig selv i at tænke. Og vi forstår godt udgangspunktet.

Reglerne kan være indviklede, svære at finde rundt i og give anledning til frustrationer. Og når man sidder med kommunikation eller marketing, kan man hurtigt tage sig selv i en følelse af, at det begrænser ens arbejde og muligheder.

Men her er det vigtigt at huske på, at reglerne er sat i verden for at passe på folks data og privatliv. Konsekvenserne ved ikke at overholde reglerne kan derfor være, at kunder og andre interessenter mister tillid til organisationen.

Derudover kan brud på reglerne medføre lange og kostbare juridiske kampe. I 2022 modtog Datatilsynet fx 8.816 anmeldelser om brud på persondatasikkerhed – og det tal har været stigende de seneste år.

Når Datatilsynet modtager disse anmeldelser, tager de stilling til, om organisationen skal indstilles til bødestraf. Og lige nu ser vi altså en tendens til, at flere og flere organisationer bliver indstillet til bøder, og at bødestørrelserne strækker sig fra alt fra 50.000 kr. til 15 mio. kr.

Det er selvfølgelig altid vigtigt at have fokus på at overholde de gældende regler. Men ofte kan man sige, at jo større en datamængde, man arbejder med, jo flere faldgruber vil der opstå ift., om man kommer til at overtræde GDPR-reglerne.

I denne guide vil vi derfor komme omkring vigtige områder, du bør have styr på, hvis du vil overholde GDPR i arbejdet med e-mails. Vi gennemgår alt fra modtagerens tilmelding til opbevaring af data helt frem til framelding.

Inden vi går i dybden, skal vi dog for en god ordens skyld nævne, at vi i Ubivox ikke er jurister. Men gennem vores daglige arbejde med nyhedsbreve, har vi de seneste 20 år opbygget en bred viden om datasikkerhed. Denne guide er bl.a. baseret på dén viden.

Samtidig er det vigtigt at nævne, at guiden udelukkende fokuserer på GDPR i forbindelse med arbejdet med e-mails og nyhedsbreve. Formålet er at gøre dig klogere på områder, du måske ikke har overvejet, i forbindelse med arbejdet med e-mails.

Der er derfor ikke tale om en fyldestgørende guide til overholdelse af GDPR generelt i organisationer.

Hvis du er i tvivl, bør du altid søge vejledning ved en jurist. Derudover er du altid velkommen til at kontakte os, så vi enten kan gøre dig klogere, eller sende dig i den rigtige retning.

God læselyst!

Før tilmelding: Fortæller vi eksplicit, hvordan vi bruger modtagerens data?

En essentiel del af GDPR er brugerens ret til at få oplyst: Hvilke data de afgiver, hvad de bruges til og hvordan de bliver slettet igen. På baggrund af det, kan vedkommende give et gyldigt samtykke til, at du må bruge disse oplysninger.

Disse informationer skal du derfor tilbyde eksplicit ved tilmeldingen til dit nyhedsbrev. Det kan enten gøres ved at linke til jeres generelle privatlivspolitik eller en separat side med nyhedsbrevsbetingelser, hvor disse informationer står tydeligt. På den måde har modtageren mulighed for at acceptere dine betingelser, når de trykker "tilmeld".

Ifølge markedsføringsloven §10 stykke 2, må du dog sende elektronisk markedsføring til kunder med tilsvarende produkter fra tidligere køb, hvis du har modtaget deres e-mailadresse i forbindelse med købet – fx i et checkout flow. Her bevæger vi os dog i en gråzone, hvor man hurtigt kan træde forkert. Det betyder nemlig, at du hele tiden skal vurdere, om indholdet i dine e-mails matcher de produkter, kunden tidligere har købt. Derfor er vores anbefaling, at du altid indhenter eksplicit accept, før du sender e-mails til en kunde. Så er du på den sikre side.

Du kan læse Datatilsynets guide til oplysningspligten her.

Er du i tvivl, om jeres privatlivspolitik indeholder de nødvendige punkter?

GDPR.dk har lavet en vejledning og skabelon til udarbejdelse af privatlivspolitik.

I privatlivspolitikken er det bl.a. vigtigt at fortælle hvilke data I samler op, hvad de bruges til og hvor hurtigt de slettes efter framelding af nyhedsbrevet.

Dobbelt opt-in giver et ekstra godkendelseslag

Udover det eksplicitte samtykke, anbefaler vi, at du opsætter en dobbelt opt-in e-mail. Altså en e-mail, modtageren får, lige efter tilmelding, hvor de skal trykke på et link for at bekræfte samtykket. Selvom det som udgangspunkt ikke er nødvendigt for at overholde GDPR, er der flere grunde til, at vi anbefaler det ekstra godkendelseslag. Hvis en modtager ved en fejl bliver tilmeldt et nyhedsbrev, bliver deres persondata opbevaret hos udbyderen uden et samtykke fra vedkommende. Her kan en opt-in mail sikre, at du kun har modtagere, der aktivt har givet et samtykke, samtidig med at du kan bevise samtykket, hvis det skulle blive nødvendigt.

Derudover anser vi dobbelt opt-in som god e-mailpraksis, der bl.a. kan være med til øge kvaliteten af dine kontakter. Det viser nemlig, at modtageren er 100 % klar over, at de har tilmeldt sig, og ofte medfører det mere aktive modtagere.

I nogle europæiske lande – herunder Tyskland – er det et lovkrav at bruge dobbelt opt-in. Hvis du arbejder med e-mails og nyhedsbreve på et internationalt plan, er det derfor vigtigt, at du har sat dig ind i, hvorvidt du skal opsætte en dobbelt-in eller ej. Den nemme løsning vil selvfølgelig være, at du konsekvent benytter dig af det.

Oplys om brug af spy pixels

Mange e-mailplatforme benytter sig af såkaldte spy pixels i forbindelse med tracking af adfærd i nyhedsbreve. En spy pixel er et skjult billede, der rapporterer til nyhedsbrevssystemet når en e-mail åbnes. Dermed kan nyhedsbrevssystemet registrere, når en modtager åbner en e-mail, så det kan blive præsenteret i statistikken.

Det er i sig selv ikke et problem, hvis man har gjort modtageren opmærksom på det ved tilmeldingen – men det er langt fra alle organisationer, der husker det. I december 2022 udtalte Datatilsynet bl.a. alvorlig kritik af Vækstfonden for hverken at indhente gyldigt samtykke eller opfylde oplysningspligten i forbindelse med brug af spy pixels i nyhedsbreve.

Vores råd er derfor: Undersøg om I bruger spy pixels i jeres e-mails. Hvis I gør, skal I oplyse om det i nyhedsbrevsbetingelserne.

Har I glemt at oplyse om tracking i jeres nyhedsbrevsbetingelser?

I Ubivox bruger vi ikke spy pixels, men vi tillader andre former for tracking. Hvis du ikke ønsker denne tracking, kan du tilvælge et addon, der slukker for trackingen, så du er på den sikre side. Alternativet er, at du skal genindhente samtykke til dine modtagere, hvor de accepterer din tracking, før du kan sende til dem igen.

Efter tilmelding: Opbevarer vi modtagerens data forsvarligt?

Når modtageren har accepteret dine betingelser for at afgive deres data, skal du selvfølgelig efterleve det, du har lovet. Foretager du ændringer ift. indsamling, opbevaring eller brug af data, skal modtageren selvfølgelig opdateres om det – og i de fleste tilfælde acceptere de nye vilkår.

Derudover er der nogle konkrete områder, du bør være opmærksom på.

Opbevar og håndtér modtagerlister forsvarligt

Når du fokuserer på at opbevare og håndtere dine modtageres data forsvarligt, viser du, at du tager deres personlige informationer alvorligt og at du agerer ansvarligt. Det første skridt er derfor at vurdere, om du din e-mailplatform bidrager til det. Du kan læse mere om valg af e-mailplatform på side 9 i denne guide.

Det næste skridt er at vurdere, hvordan du håndterer eksporterede modtagerlister.

Der kan nemlig være mange årsager til, at man eksporterer en modtagerliste fra e-mailplatformen. Det kan fx være for at flytte den til et andet system, for at berige den og uploade den igen eller noget helt tredje. Men du skal være opmærksom på, at du kan løbe ind i problemer, hvis du gemmer filerne usikre steder – fx steder som andre kan tilgå eller i ikke-compliant systemer og cloud-løsninger.

Det kan bl.a. være et problem, hvis din computer bruger OneDrive og du har slået automatisk lagring til i mappen, hvor filen gemmes, hvis andre personer kan tilgå mappen. Når listen automatisk gemmes i en cloud, som andre personer (fx kollegaer) kan tilgå, er der nemlig ikke tale om forsvarlig håndtering af modtagerens persondata, hvis disse personers adgang til dataet ikke er relevant for deres arbejde.

Du kan med fordel slå automatisk lagring fra på computerens skrivebord og gemme eksporterede lister der. Når arbejdet er færdigt, skal du selvfølgelig slette listen fra enheden. Husk derefter at tømme papirkurven.

Sørg for nem framelding

Ifølge markedsføringsloven skal en nyhedsbrevsmodtager til enhver tid have mulighed for at framelde dit nyhedsbrev. Derfor skal du altid have et tydeligt frameldingslink – fx i bunden af dine e-mails.

Når en modtager framelder dit nyhedsbrev, skal du ikke se det som et nederlag. Det er bedre, at de selv framelder, end at de bliver på listen som inaktive modtagere eller ultimativt set anmelder en af dine e-mails for spam, og skader dit afsenderomdømme.

Hvis du arbejder med flere lister, bør du gøre det klart for modtageren, hvorvidt de framelder alle lister, de er tilknyttet, eller om de skal afkrydse hver liste manuelt for at framelde dem individuelt.

Ved siden af linket til framelding kan du samtidig overveje have et link til din privatlivspolitik, så modtageren altid kan tilgå denne side nemt og enkelt.

Framelding: Sletter vi modtagerens data, når de beder om det?

Når du arbejder med e-mails og nyhedsbreve, er det vigtigt, at du forholder dig til, hvordan du håndterer frameldinger. Først og fremmest skal det selvfølgelig være nemt for modtageren at framelde sig. Udover at der er tale om god service, er et tydeligt frameldingslink i din e-mail samtidig et af kriterierne for, at din e-mail ikke ender i spammappen. Derudover er frameldingen med til at opfylde et vigtigt aspekt af GDPR: Personers ret til at få slettet deres data.

Overhold modtagerens right to be forgotten

En af grundstenene i GDPR-reglerne er personers "right to be forgotten". Altså deres ret til, at du sletter deres personhenførbare data, når de beder om det. Udgangspunktet er nemlig, at personer selv ejer deres data, og at du kun låner det i dit arbejde. Når du ikke længere skal bruge det, skal det derfor slettes.

I de fleste e-mailplatforme slettes modtageren automatisk fra listen, når de framelder sig nyhedsbrevet. Men det betyder ikke, at alt deres personhenførbare data er slettet. Nogle platforme gemmer oplysningerne i en vis periode som backup. Andre systemer gemmer dem til fremtidig brug – hvad nu hvis modtageren tilmelder sig igen? Og så er der organisationer, der aktivt har lavet lister, hvor modtagere flyttes hen, når de framelder sig.

I Ubivox har vi lavet en specifik funktion til at håndtere på modtagerens right to be forgotten. Det eneste du skal gøre for at slå den til, er:

1. Gå til "GDPR-indstillinger" under fanen "Konto"
2. Opsæt dine kriterier for den automatiske RTBF
3. Du skal ikke længere bekymre dig om, hvorvidt du overholder dit juridiske ansvar ift. dine modtageres ret til at få slettet deres data

Vores anbefaling er, at du undersøger, om jeres platform og opsætningen af jeres konto overholder modtagerens "right to be forgotten". Hvis ikke, bør I selvfølgelig sørge for, at det sker.

Oprydning af lister

Hvis dine modtagere ikke interagerer med dine e-mails, kan de være med til at skade dit afsenderomdømme. E-mailklienterne ser nemlig på, hvor meget interaktion du har i din e-mailindsats. Er den for lav, giver det minuspoint i bogen, og øger risikoen for at fremtidige e-mails ender i spammappen.

Ligesom med dobbelt opt-in, er oprydning af lister ikke et decideret krav ift. GDPR. Det er dog værd at nævne, fordi du gør noget aktivt ift. at have en modtagerliste med personer, der faktisk anser dit indhold som relevant. Udover at påvirke dit afsenderomdømme positivt, kan det være med til at minimere mængden af spamklager og frameldinger.

Sådan rydder du op i dine lister

1. Opsæt e-mail automation til modtagere, der ikke har åbnet en e-mail i X-periode. Lav en interessant og anderledes emnelinje, der øger sandsynligheden for, at modtageren åbner e-mailen. Gør modtageren opmærksom på, at de bliver fjernet fra listen, hvis de ikke klikker i din e-mail. Fokusér derudover på værdien af dit nyhedsbrev, for at overbevise dem om at blive.

2. Opsæt e-mail automation 2, der sendes til personer, der ikke klikkede i e-mail 1 inden for 3 dage. Fortæl modtageren, at de bliver fjernet inden for 48 timer, hvis de heller ikke klikker i denne e-mail.

3. Opsæt e-mail automation 3, hvor du siger tak for denne gang og fortæller, at modtageren altid er velkommen til at tilmelde sig igen (og opnå alle dine fordele i nyhedsbrevet).

4. Opsæt en medlemshandling, der fjerner modtagere, der hverken har klikket i e-mail 1 eller 2.

Fremtiden for GDPR i e-mailverdenen

Generelt ser vi et større og større fokus på persondatasikkerhed både i Danmark og i udlandet. Det kan bl.a. ses på Googles udfasning af tredjepartscookies og Apples privacy protection foranstaltninger, der allerede startede med iOS 15-opdateringen i 2021. Begge er et skridt mod en fremtid, hvor indsamling af personers online fodaftræk i højere grad begrænses.

Samtidig kan det stigende fokus på persondatasikkerhed ses på Datatilsynets arbejde med at undersøge og vurdere virksomheders overholdelse af GDPR. Siden 2018 har Datatilsynet nemlig indstillet 35 virksomheder og offentlige instanser til bøder på baggrund af brud på GDPR (pr. marts 2024) – og antallet af bøder er stigende.

Schrems' udfordring af EU/US aftalen

Det er ingen hemmelighed, at der har været store udfordringer mellem EU og USA i forbindelse med persondatasikkerhed efter EU introducerede GDPR.

Den største udfordring er lovbestemmelsen, FISA 702, der betyder, at den amerikanske regering kan tilgå og overvåge data fra amerikanske virksomheder og deres kunder, hvis der er mistanke om, at disse personer har planer om kriminelle aktiviteter, der kan skade USA.

Og det er et problem for europæiske virksomheder, fordi de derfor ikke kan opbevare og behandle persondata i amerikanske systemer og samtidig overholde GDPR.

Det var bl.a. en af årsagerne til, at Datatilsynet i 2022 konkluderede, at man ikke kunne bruge Google Analytics uden supplerende foranstaltninger.

Derfor har EU og USA tre gange forsøgt at lave en aftale, der skal komme dette problem til livs. De to første forsøg blev erklæret ugyldige efter den østrigske advokat, Max Schrems, udfordrede aftalerne og fik medhold ved EU-Domstolen.

Den tredje aftale mellem EU og USA kom på plads i sommeren 2023. På baggrund af den, er det muligt at bruge amerikanske systemer, der er certificeret under EU-U.S. Data Privacy Framework.

Men som med de to forudgående aftaler har Max Schrems endnu engang planer om at udfordre aftalen. Og meget tyder på, at denne aftale også bliver erklæret ugyldig. Dette bliver vi formentlig klogere på i løbet af 2024. I skrivende stund (marts 2024) er aftalen dog stadig gyldig.

Vælg en sikker platform

Hvis den nuværende aftale mellem EU og USA bliver erklæret ugyldig, betyder det, at amerikanske systemer, der behandler personoplysninger og persondata, igen bliver non-compliant. Og derfor skal du forholde dig til dit valg af platform, hvis du vil overholde GDPR – er platformen amerikansk eller bruger den underdatabehandlere i USA?

Når du vælger e-mailplatform – og i øvrigt også andre relevante systemer til håndtering af persondata, fx CRM-systemer – har platformens niveau af datasikkerhed direkte indflydelse på din organisations håndhævelse af GDPR. Her opbevares og behandles modtagerens data nemlig, når de har tilmeldt sig. Et brud på systemet vil dermed få direkte konsekvenser for jer.

Desværre findes der mange systemer, der bryster sig af at være GDPR-compliant, som egentlig ikke er. Når man undersøger dem nærmere, har de måske en databehandler i andet led, der ikke helt er compliant. Og det betyder, at de heller ikke er compliant. Derfor bør I altid foretage en grundig vurdering af de systemer, I bruger i arbejdet med datahåndtering.

Brug din e-mailindsats til indsamling af førstepartsdata

Som nævnt ovenfor, bliver det svære for organisationer at gøre brug af tredjepartscookies i markedsføring i fremtiden. Og det peger mod, at man i højere grad er nødsaget til at fokusere på førstepartsdata i forbindelse med markedsføring – altså data man selv indsamler og selv ejer.

Og her spiller e-mails og nyhedsbreve en stor rolle. Når du indsamler informationer om dine modtagere og kunder i forbindelse med din e-mailindsats, er der nemlig som udgangspunkt tale om førstepartsdata. Det kan fx være, at du får registreret datapunkter som modtagerens adfærd med dine e-mails, deres køb hos dig eller at de selv får mulighed at udfylde stamdata og interesser (fx ved tilmelding).

En af fordelene ved førstepartsdata er, at du selv styrer spillereglerne. Du er ikke afhængig af ændringer, begrænsninger eller stigning i annoncepriser fra eksterne spillere som Google og Facebook. I takt med, at der kommer flere og flere ændringer på området, bliver det derfor kun vigtigere, at du starter din indsats med at indsamle og bruge førstepartsdata.

Hvis du vil blive klogere på, hvordan du indsamler og bruger førstepartsdata, har vores kollegaer fra Heyloyalty skrevet et blogindlæg om emnet. Du kan læse blogindlægget her.

Få adgang til en dansk GDPR-compliant e-mailplatform – ligesom +1.000 danske virksomheder og offentlige instanser

I Ubivox har vi stort fokus på GDPR og datasikkerhed. Derfor har vi hele tiden en finger på pulsen ift. ændringer på området. Vi mener nemlig, at du skal kunne koncentrere dig om din kommunikation, uden at være nervøs for om dit e-mail system er GDPR-compliant. Vi rådgiver og vejleder derfor løbende vores kunder inden for GDPR i forbindelse med deres e-mailindsats.

Du kan altid prøve vores platform – det er gratis, så du selv kan vurdere, om det er tid til at skifte platform.

FÅ DIN GRATIS DEMO I DAG

E-mail og automatiserede kampagner

Sælg flere produkter, lav tidsbaserede online kurser, interne vidensforløb eller sørg for at fastholde kunder med produktviden.

Nyhedsbreve og information

Giv information og viden til jeres kunder og opdatér medarbejdere i organisationen om nye tiltag.

Transaktionelle og 1-til-1 e-mails

Få effektiv levering og overvågning af ordrebekræftelser, fakturaer og 1-til-1 forsendelser med nem integration via SMTP.

Fleksible sporingsmuligheder

Vælg selv hvor meget aktivitet, du vil spore i dine e-mails, så du sikrer, at du har de rigtige data til rådighed.