Zenta Creative presenterar

GDPR GUIDEN

zenta

CURIOUS HEART. DIGITAL MIND.

Välkommen till GDPR-Guiden!

Hej!

Vi på Zenta har sedan GDPR's inträde 2018 hjälpt många av våra kunder och partners med GDPR-anpassade texter för nyhetsbrev, webbplatser och e-handelslösningar.

Vilka är vi?

Vi brinner för digitalisering och jobbar på att skapa nästa generations digitala verktyg som förenklar och förbättrar människors livskvalitet. Våra superkrafter är vår enorma handlingskraft, nyfikenhet och orädda arbetssätt. Vi har kunskaper från olika branscher med allt från automotive till spel. Det ger oss möjlighet att överföra vår expertis från en bransch till en annan där vi på ett effektivt sätt kan skapa innovativa lösningar.

Nu har vi skapat en lättsmält guide för dig som på något sätt kommer påverkas av GDPR, om du ska skicka ut nyhetsbrev eller behöver samla in uppgifter från kunder.

På Datainspektionens hemsida hittar du fördjupningar inom just ditt område om du skulle behöva.

"Som företag har du alltid det yttersta ansvaret, med denna enkla guide har du den grund du behöver för att på ett säkert sätt kontakta dina kunder."

- Aida

Kommunikationschef

Vad är GDPR?

GDPR är en dataskyddsförordning som verkar för att skydda enskilda personers grundläggande rättigheter och friheter samt deras rätt till skydd av personuppgifter. Dataskyddsförordningen gäller på samma sätt i hela EU.

Alla lagar och regler gällande personuppgifter kan du hitta på Datainspektionens hemsida.

Vad är en personuppgift?

Personuppgifter är den information som kan knytas till en levande person, såsom namn, adress och personnummer samt foton. Även ljudinspelningar som lagras digitalt kan vara personuppgifter, helt enkelt allt som kan identifiera en person. Registreringsnummer på en bil som tillhör en privatperson är en personuppgift men inte en firmabil som används av flera personer i ett företag. Även om en e-post kan vara en anonym adress, så kan den nästan alltid knytas till en person.

E-post som skickas till flera mottagare rekommenderas enligt GDPR att skickas som dold kopia (BCC).

Personuppgifter om barn är särskilt skyddsvärda i dataskydds-förordningen eftersom barn kan ha svårare att förutse riskerna med att lämna ifrån sig uppgifter och sina rättigheter. För att hantera personuppgifter om barn under 16 år krävs vårdnadshavares samtycke. Denna ålder varierar mellan 13 och 16 beroende på land, i Sverige gäller 13.

Vad är INTE en personuppgift?

Ett bolagsnummer är ofta inte en personuppgift men kan vara det om det handlar om ett enmansföretag eller enskild firma där organisationsnumret också är personnumret.

Datainspektionens rekommendationer:

- När ni mottagit och läst e-posten, bedöm om uppgifterna ska bevaras och var.
- Skicka inte känsliga personuppgifter i oskyddad e-post.
- Informera på er webbsida i samband med e-postadressen hur ni behandlar personuppgifter eller länka till er integritetspolicy.
- Om ni skickar svar eller autosvar, bifoga en standardtext där ni informerar den som skickat e-post om hur ni behandlar personuppgifter eller länka till en integritetspolicy på er webbplats.
- Informera alla i er organisation om reglerna och rutinerna för hur ni behandlar personuppgifter i er organisation.
- Håll rutinerna levande.

Vad är cookies?

"Webbplatser du besöker sparar textfiler på din dator för att t.ex. ge tillgång till olika funktioner eller för att spåra hur du surfar på webbplatser.

Cookies är till fördel för webbplatser och därför ska det ingå i din integritetspolicy hur du hanterar dessa."

Särskild personlig information

"Särskild personlig information gäller en individs politisk inriktning, hälsa, sexuell läggning, religion eller tro, etnicitet, medlemskap i en professionell organisation eller brottsregister."

Vad behandlas under GDPR?

Att "behandla" innefattar alla åtgärder som rör personlig information, t.ex. att lagra information, vidarebefordra den till en annan part eller att ha tillgång till informationen.

Det innebär att i samband med e-postmarknadsföring behandlar du personlig information så fort du använder denna data på något sätt alls.

Integritetspolicy

Företag måste ha en integritetspolicy. Det är en text på din webbsida som berättar hur ditt företag hanterar besökarnas, prenumeranters och kunders personuppgifter.

Du kan ladda ner Zentas integritetspolicy på zenta.se/guider. Notera att beroende på din bransch, krav på personuppgifter och hantering av dessa kan du behöva göra tillägg till mallen för att anpassa helt till ditt företag.

Registreringsprocess

Registreringen är en process som varje prenumerant går igenom, oftast via din webbsida eller en landningssida. Dina prenumeranter lämnar sina uppgifter så som e-postadress, namn eller annan personlig information under registreringsprocessen för t. ex. ett nyhetsbrev.

Här är det viktigt att förstå vad som räkna med personlig information så att man som digital marknadsförare kan samla in och hantera information på rätt sätt.

Personlig information enligt GDPR

Personlig information är all information som kan identifiera en fysisk person, t.ex ett namn eller en bild, e-postadress, IP-adress eller cookie-ID.

Pseudonymiserad information där man försökt att anonymisera information så en hashad-IP-adress anses också vara personlig information eftersom det är möjligt att identifiera personen i fråga även om det kan kräva lite jobb genom att kombinera databaser.

Din roll som marknadsförare

Beroende på din roll finns det olika GDPR-krav på dig som du måste bemöta.

- **Den ansvariga parten** - den som beslutar att behandla personuppgifter för ett visst syfte och definierar syftet och de resurser som ska användas
- **Den berörda parten** - den fysiska person vars personuppgifter behandlas.
- **Processorn** - som ska möjliggöra hantering av personuppgifter, t.ex. ”stödja” eller genomföra personuppgiftshantering.

Många väljer att använda sig av en ESP, vilket är klokt då det ses som mer professionellt och du får enkelt möjlighet att erbjuda dubbel opt-in för prenumeranter samt avregistreringsmöjligheter. Dubbel opt-in är när prenumeranten behöver gå in på sin mail för att verifiera att de vill prenumerera.

ESP
E-mail service provider

“ESP är en e-posttjänst för massutskick av e-mail, såsom nyhetsbrev.”

Om du väljer att använda en ESP för att skicka nyhetsbrev gör det dig till ansvarig för den data du hanterar om de prenumeranter som registrerar sig. Du är alltså en ansvarig medan ESP’n är processorn och prenumeranten är den berörda personen.

Det är juridiskt nödvändigt att upprätta skriftliga avtal mellan den ansvariga parten och processorn. Avtalet täcker t.ex. vad processorn kan göra med informationen, hur processorn ska hålla din data säker och hur båda parter kommer att hantera eventuella dataläckor och de berörda personernas rättigheter. Dessa punkter måste registreras i ett så kallat processoravtal eller personuppgiftsbiträdesavtal.

Att samla in personuppgifter

Du behöver alltid ha en legitim anledning till att samla in personuppgifter. Några anledningar är t.ex för att skriva avtal eller offert. Tillstånd att samla in personuppgifter kan bli särskilt viktigt under några fall.

Det innebär att ge tillstånd måste vara en tydlig aktiv åtgärd, t. ex. en kryssruta som personen själv klickar i. Otillåtet är numera att man automatiskt blir inlagd i ett nyhetsbrev genom att man handlar något på en webbplats. Informationen måste vara tillräckligt specifik för att individer ska veta exakt vad de ger tillstånd för och vad de kan förvänta sig av dig.

Så när de klickar i rutan för nyhetsbrev ska de veta exakt hur du kommer att använda den informationen, t.ex hur ofta du ämnar skicka mail till dem, ifall de du kommer att dela deras e-postadress med dina kunder eller leverantörer.

Av denna anledning bör du alltid hänvisa till din Integritetspolicy när du vill samla in personuppgifter.

Ett annat krav är att personen alltid ska kunna få sin data raderad och de ska på ett enkelt och tydligt sätt få veta hur de kan avsluta nyhetsbreven och att du inte längre lagrar deras uppgifter.

Du måste därför inkludera ett opt-out-alternativ i varje kommersiellt meddelande.

Tillstånd

Giltigt tillstånd enligt GDPR måste vara ett ”fritt givet, specifikt, informerat och otvetydigt uttryck av vilja”.

Dessutom måste du, som den ansvarige parten, kunna bevisa att du fått tillstånd att samla in personuppgifter från prenumeranter eller de personer du fått uppgifter från.

Visste du att ..?

GPDRs straffavgift
vara 20 miljone
bolagets globala års
beroende på vilket

t kan som mest
er euro eller 4% av
omsättning,
belopp som är högst.

Befintliga kunder

Olika länder har olika telekommunikationslagar. Vanligtvis får du skicka e-post till kunder för att marknadsföra produkter och tjänster som liknar vad de redan köpt från dig, även om de inte uttryckligen gav dig tillstånd att göra det efter att GDPR införts.

Däremot måste du först informera dina kunder om din avsikt att skicka dem dessa meddelanden, hur ofta du kommer att göra det, på vilket sätt och vad e-posten kommer att innehålla. Och som tidigare nämnt, du måste erbjuda dem ett opt-out-alternativ innan du skickar dem kommersiella meddelanden. Ny lagstiftning om integritet utarbetas och omarbetas hela tiden.

Denna europeiska lagstiftning kommer att komplettera GDPR och innehålla särskilda regler som gäller t.ex. användningen av cookies och utskick av kommersiella meddelanden. Alla nya regler är inte på plats än och det är därför klokt att hålla koll på de senaste ändringarna inom e-sekretessförordningen.

Registreringsprocessen

Det bästa sättet att sätta upp sin registreringsprocess är via en fler-stegs-metod:

Steg 1 - Lämna information

Steg 2 - Bevilja tillstånd

Steg 3 - Bekräfta tillstånd

Registreringstexten

Registreringstexten är den text som folk läser och behöver samtycka till när de ger dig sina personuppgifter. I denna text presenterar du vilken information du behöver för att kunna kommunicera med dem. Denna text är en viktig del av ett giltigt tillstånd.

Det måste enligt GDPR vara ett ”fritt givet, specifikt, informerat och otvetydigt uttryck av vilja” som kräver en aktiv åtgärd. Texten behöver därför vara tydlig, specifik och enkel att förstå. Tiden är förbi då otydliga, halvt dolda små texter räknas som villkor. Du behöver tydliggöra för prenumeranterna vilken typ av innehåll de kan förvänta sig och hur ofta.

Registreringstext och bevis

När du behandlar personuppgifter baserat på tillstånd måste du kunna bevisa att du har fått detta tillstånd. Det är smart att koppla bevisbördan för din registreringstext till ett bekräftelsemail, ett så kallat dubbel opt-in där du i bekräftelsemailet upprepar det som mottagaren ger sitt tillstånd för.

GDPR kräver inte dubbel opt-in men det gör ditt arbete som marknadsförare enklare då det ger dig de bevis du behöver och prenumeranten måste verifiera sin epostadress. Det är alltså rekommenderat att använda dubbel opt-in för att eliminera osäkerheter.

Lagring av din registreringstext

Du bör lagra din registreringstext och den tillåtelse du får från prenumeranter. För att kunna göra det på ett bra sätt kan du ta hjälp av checklistan nedan.

Checklista:

- Förklara vem som ska kommunicera (du, en tredje part eller ett annat företag).
- Förklara vilken information du ska använda och varför.
- Förklara vilken kanal du ska använda för att skicka din information.
- Förklara hur ofta du skickar dina meddelanden.
- Länka till integritetspolicyn och förklara att prenumeranterna kan hitta mer information där. Se till att din integritetspolicy är GDPR-säker.
- Be om separat tillstånd för varje specifikt syfte för vilket du planerar att använda personuppgifterna.
- Se till att du har bevis på den tillåtelse som prenumeranten ger dig. Du bör också spara registreringstexten som folk samtyckte till.
- Se till att det är lika enkelt för prenumeranterna att återkalla sitt tillstånd som det var att ge det. Du inkluderar därför ett opt-out-alternativ i varje meddelande du skickar.
- Inkludera en avprenumerera-länk i varje kommersiellt e-post-meddelande.
- Observera att du måste uppfylla ytterligare krav om dina mottagare är under 16 år eller om du behandlar särskild personlig information.
- Ta reda på vad som gäller för ditt specifika fall om du hanterar särskild personlig information.

Exempel på en registeringstext

Här är ett exempel på en registreringstext så att den som ska registrera sig vet vem som ska skicka ut information, varför, hur och hur ofta. Du kan använda denna text och ändra till ditt företagsnamn samt information om hur utskick ska göras.

”Du får detta nyhetsbrev av Zenta för att du registrerat dig på våra nyhetsbrev. Du kan när som helst avprenumerera genom att klicka på ”avregistrera” längst ner i nyhetsbreven.

Vi använder bara ditt namn och e-postadress för att skicka dig nyhetsbrev om nya tjänster, nyheter du kan ha nytta av, produkter eller erbjudanden. Våra utskick kommer ca 2 gånger i månaden via e-post, vi skickar inte ut någonting via sms eller brev. I vår Integritetspolicy kan du se hur vi hanterar dina personuppgifter och hur du kan göra om du helt vill bli raderad från våra listor.

Vi gör inga andra utskick eller lägger till dig på andra listor utan tillstånd. Ifall du vill prenumerera på andra tjänster, vänligen registrera dig till den separata tjänsten. Du kommer att få ett mail som du verifierar genom att klicka på länken så att vi får ditt godkännande.

För att prenumerera behöver du vara över 16 år eller ha vårdnadshavares godkännande.

Snabb-quiz för GDPR

- ☐ Har du kundlistor?
- ☐ Har du leverantörslistor?
- ☐ Har du anställda?
- ☐ Skickar du nyhetsbrev eller någon form av reklam till dina kunder?
- ☐ Har du en lista över vilka personuppgifter ditt företag hanterar?
- ☐ Har du en beskrivning på hur du använder dessa uppgifter?
- ☐ Använder du dig av något bokningssystem?
- ☐ Sparar du anställdas personuppgifter i ett lönesystem?
- ☐ Har er webbplats bilder och/eller kontaktuppgifter till de anställda?
- ☐ Har ni en policy om hur länge ni sparar kunders, anställdas och leverantörers uppgifter?
- ☐ Har ni en policy på hur ni skyddar uppgifter om de anställda, leverantörer och kunder?

Svarade du JA på allt?
Då har du redan bra koll på GDPR.

I grund och botten handlar det om att skydda människors uppgifter och inte skicka ut reklam som människor inte vill ha.

Ifall något är oklart, tänk alltid att det ska vara till privatpersoners fördel och ta det säkra före det osäkra. Du får till exempel inte samla in uppgifter om människor utan deras vetskap eller godkännande och de ska alltid få välja att bli raderade från dina listor och system.

Frågetecken eller funderingar?

Vi här på Zenta älskar att prata om digitalisering och olika utmaningar som företag kan ställas inför.

Hör av dig till oss !

Scanna mig!

zenta

CURIOUS HEART. DIGITAL MIND.

zenta

CURIOUS HEART. DIGITAL MIND.