AVG in de praktijk, tips!

Google Analytics
Zo kun je Google Analytics gebruiken zonder cookie melding.

- Accepteer het “Amendement gegevensverwerking” in je Analytics-account (‘Beheer’ > ‘Account instellingen’ en dan helemaal onderaan);
- Blokkeer het meezenden van volledige IP-adressen (ga(‘set’, ‘anonymizeIp’, true);) en forceer tevens SSL (ga(‘set’, ‘forceSSL’, true););
- Zet het delen van gegevens met Google uit (‘Beheer’ > ‘Account instellingen’ en dan vier instellingen uitvinken);
- Informeer je bezoekers in een cookieverklaring of privacyverklaring over je gebruik van Google Analytics.

https://support.google.com/analytics/answer/3379636?hl=nl

Voor het plaatsen en uitlezen van functionele cookies is het verkrijgen van voorafgaande toestemming niet vereist.

Cookies waar wel toestemming voor moet worden gevraagd

- Cookies waarmee je individueel klikgedrag meet (o.a. HotJar).
- Cookies waarmee je meet hoe lang iemand op een pagina is (om daarna bijvoorbeeld een livechat te kunnen openen).
- Cookies waarmee je bezoekers laat reageren via social media.
- Cookies om te meten of iemand een advertentie heeft gezien.

Deze toestemming is 12 maanden geldig

Rechten van betrokkenen
Gebruikers hebben recht op inzage en verwijdering. Als een klant vraagt om verwijdering, moet je hier in de meeste gevallen binnen een maand gehoor aan geven.

Overzicht verwerkingen
Maak een overzicht van al je verwerkte persoonsgegevens. Noteer waar je de data vandaan

hebt, met welk doel je ze hebt opgeslagen en met wie je ze deelt. Zorg dat je ook vermeldt op basis van welke wettelijke grondslag je deze gegevens verwerkt.

Privacy Impact Assessment (PIA)
Het wordt ook verplicht om een Privacy Impact Assessment (PIA) uit te voeren als je data verwerkt met een hoog privacyrisico. De PIA is een instrument waarmee je vooraf kunt bepalen wat risico's zijn die horen bij het verwerken van bepaalde persoonsgegevens.

Privacy by default
Privacy by default wil zeggen dat je technische en organisatorische maatregelen moet nemen waardoor je standaard uitsluitend de strikt noodzakelijke gegevens verzamelt voor het specifieke doel.

Functionaris voor de gegevensbescherming
Als je bedrijf op grote schaal persoonsgegevens verwerkt en dit je kernactiviteit is, ben je verplicht een functionaris voor de gegevensbescherming aan te stellen. Ook overheidsinstanties en publieke organisaties moeten zo'n functionaris hebben.

Meldplicht datalekken?
De meldplicht datalekken is niet nieuw. Bij de AVG is het echter de bedoeling dat je alle datalekken vastlegt op een manier waarop de Autoriteit Persoonsgegevens precies kan zien of je genoeg hebt gedaan aan het beschermen van de gegevens.

Monitor je het individuele klikgedrag van mailontvangers?
Dan moeten ze hier expliciet toestemming voor geven. Een goed argument is dat je op basis van deze informatie relevantere mailings kunt sturen.

Toestemming
De AVG legt strengere regels op omtrent de manier waarop je toestemming vraagt, krijgt en registreert. Je klanten moeten een geldige toestemming geven en deze eenvoudig weer kunnen intrekken. Controleer je formulieren goed en pas ze zonodig aan.
Houd alle verzamelde gegevens ook niet langer in huis dan nodig is voor het beoogde gebruik.

Vanaf 25 mei 2018 heb je documentatieplicht. Dit wil zeggen dat je moet kunnen aantonen dat je technische en organisatorische maatregelen hebt genomen om aan de AVG te voldoen.

Automatisch ingevulde optin vakjes zijn definitief verleden tijd.

Wat zijn 'persoonsgegevens'?
Naam
Adres
Telefoonnummer
E-mailadres

IP-adres
Geboortedatum
Geslacht
Schoenmaat
KlantID
OrderID
GebruikersID
Versleuteld e-mailadres

Minstens net zo belangrijk is dat je kunt verantwoorden hoe en wanneer je toestemming hebt gekregen van een betrokkene om zijn of haar specifieke persoonsgegevens te gebruiken.
Een manier om dit vast te leggen is in een CRM-systeem. Daarin staat dan met een timestamp aangegeven wanneer iemand toestemming gaf. Ook de manier van toestemming geven moet worden worden vermeld.

Wat moet er in de privacyverklaring staan?
- Welke persoonsgegevens je verwerkt.
- Met welke doelen je deze gegevens verwerkt.
- Of hier een wettelijke basis voor is (bijvoorbeeld bewaarplicht).
- De bewaartermijn voor elk soort persoonsgegeven.
- Met welke derde partijen je persoonsgegevens deelt.
- Hoe de betrokkene een klacht kan indienen bij het AP.
- Hoe je toestemming vraagt voor het krijgen van persoonsgegevens.
- Dat betrokkenen hun toestemming altijd mogen intrekken.
- Hoe betrokkenen hun persoonsgegevens altijd mogen inzien.
- Hoe betrokkenen hun persoonsgegevens altijd mogen wijzigen.
- Hoe betrokkenen hun persoonsgegevens altijd mogen verwijderen.
- Hoe betrokkenen hun persoonsgegevens altijd mogen meenemen.
- Naam en contactgegevens van de verantwoordelijke persoon bij je organisatie voor privacy- en gegevensbescherming.

Voorbeeld: https://www.consumentenbond.nl/over-ons/voorwaarden-en-privacy/privacy/privacyverklaring

Wat moet er in een verwerkersovereenkomst staan?
- Ook het soort persoonsgegevens zet je in de overeenkomst.
- Verwerking vindt plaats op basis van jouw schriftelijke instructies.
- Uitbesteding aan subverwerkers mag alleen na jouw toestemming.
- De verwerker gebruikt de persoonsgegevens niet voor eigen doeleinden.
- Mensen werkzaam bij/voor de verwerker hebben een geheimhoudingsplicht.
- Welke passende beveiligingsmaatregelen de verwerker neemt.
- Hoe de verwerker betrokkenen helpt met hun privacyrechten.
- Na de werkzaamheden worden persoonsgegevens weer verwijderd.
- Dat de verwerker desgevraagd meewerkt aan audits.

Voorbeeld:
https://www.privacycompany.eu/files/Format%20Verwerkersovereenkomst%20Standaard.pdf

Wat moet er in een register verwerkingsactiviteiten staan?

- Naam en contactgegevens van je organisatie/vertegenwoordiger.
- Eventuele andere organisaties waar je persoonsgegevens mee deelt.
- De doelen waarvoor je persoonsgegevens verwerkt.
- Een beschrijving van de categorieën van persoonsgegevens.
- Datum waarop je de gegevens moet wissen (als dat bekend is).
- De categorieën van ontvangers aan wie je persoonsgegevens verstrekt.
- Of je gegevens met een land/organisatie buiten de EU deelt.
- Een beschrijving van de technische en organisatorische maatregelen die je hebt genomen om persoonsgegevens die je verwerkt te beveiligen.

Verantwoordelijke voor de gegevensverwerking:
afkorting:
Alias:
adres:
statuut:
algemeen telefoonnummer:
algemeen e-mailadres:
website:
Functionaris voor de gegevensbescherming:
adres:
telefoonnummmer:
GSM:
e-mail:
behoort tot personeel:

-

Tot slot

Kleinere ondernemers kunnen erin volstaan om de rechten te noemen in hun privacyverklaring en consumenten de mogelijkheid te geven met specifieke verzoeken te mailen. Grotere partijen zullen het lastig gaan krijgen om alle verzoeken handmatig te beantwoorden.

1. Doe een nulmeting. Welke gegevens verwerk je nu al?
2. Verwerk alleen noodzakelijk gegevens. Privacy by design.
3. Bewaar persoonlijke gegevens niet te lang.
4. Cookies? Vraag eerst netjes om toestemming.
5. E-mails? Vraag weer netjes om toestemming.

6. Pas je privacyverklaring en cookie statement aan.
7. Sluit verwerkersovereenkomsten af.
8. Stel een register verwerkingsactiviteiten op.
9. Toon aan dat je toestemming hebt van de betrokkene.
10. Zorg voor recht op inzage, wijzigen, portabiliteit en vergeten.
11. Maak een databeveiligingsbeleid/scherp het aan.

Heb je nog vragen?
Neem dan contact met FBI design op! privacy@fbidesign.nl of bel: 023 – 531 29 77