

GDPR, Is het dat maar?!

Thomas Ghys

11 april 2018

Thomas Ghys - If it's not yes, it's NO

- GDPR prioriteiten voor elk bedrijf
 - Awareness
 - Data register
 - Juridische basis
 - Juridische documenten
 - Rechten van het individu
 - Gegevensbescherming
- Voorbeeld
 - Data register Mailchimp



GDPR prioriteiten voor elk bedrijf

#1 Awareness & training

- Deel de belangrijkste principes achter GDPR
- Leg uit waar werknemers rekening mee moeten houden

#2 Data register

- Lijst de belangrijkste processen, applicaties, databases en vendors op
- Doe een pragmatische data mapping (bv. via template en aanbeveling CBPL) ook al zijn er nog veel open vragen
- Spendeer vooral tijd aan risicovolle processen en vendors

#3 Juridische basis

- Ga na dat voor elk proces je bedrijf een geldige juridische basis heeft (typisch contract, toestemming of gerechtvaardigd belang)

GDPR prioriteiten voor elk bedrijf

#4 Juridische documenten

- Updaten van privacy policy en opstellen/aanvaarden van verwerkingsovereenkomst zijn **MUST**
- Je advocaat of vaste jurist kunnen hierbij helpen

#5 Rechten van individu

- Zet manueel proces op om individu verzoeken te laten sturen (bv. via privacy@company.com vermeld in privacy policy)
- Zorg voor interne procedure met verificatie identiteit, validatie geldigheid vraag, verduidelijking van wat individu wil weten, en opvolging om te antwoorden binnen 30 dagen

#6 Gegevensbescherming

- Prioritiseer duidelijke zwaktes in gegevensbescherming (zie verder)
- Documenteer deze analyse en de planning van initiatieven die pas na mei 25 uitgevoerd kunnen worden

Voorbeeld proces data register

Process	newsletter
Processor	Mailchimp
Description	data subjects interested in receiving our newsletters directly provide their personal data to Mailchimp via the online subscription form. This information then remains as a saved distribution list in the Mailchimp system. Every Mailchimp database is based on an opt-in emailing service with a subscription form. Once a registration is submitted by the user, the system stores the data provided by the person as a new entry in the database and notifies the person about this action via the email address that was provided during the opt-in registration. This and all subsequent emails from the service contain a one-click opt-out mechanism
Purpose	the purpose of the data collection and processing is to allow the distribution of event invitations, announcements, relevant information and several newsletters
Basis	consent
Data subjects	customers, members or subscribers
Data fields	name, email, job title, organization, residential address, language of preference, newsletter interests
Special data fields	none
Storage	Mailchimp servers located in US
Retention	for duration of subscription; personal data of an individual withdrawing consent are removed within 14 days. A unique identifier is used to keep the individual in a "do not contact list"
Recipients	designated members involved in managing the sending and the analysis process for the newsletter; administrator responsible for the regular backup of the distribution list
Transfer	Mailchimp servers through Privacy shield
Safety	see Mailchimp privacy policy