ANALYST BESPOKE CONTENT

WELL ENCRYPTED

Marketing campaigns under the sign of the GDPR

THE GROUP OF ANALYSTS

ANALYST BESPOKE CONTENT

BY ANDRES DICKEHUT

Security in dealing with personalised data plays a new and major role today. As a company driving marketing, how do I process these data? Which data may I save, for how long, and for what purpose? The GDPR also gives marketers an opportunity to build and expand upon customer confidence. But this opportunity exists alongside the requirements of the Regulation that must be fulfilled. Legally compliant e-mail marketing automation can offer marketing departments considerable assistance in meeting these requirements.

The keys to campaign success are client-specific customer contact, personal service, feedback and custom actions. But the gateway to customer trust only opens if consumers have the feeling that their data are in good hands. Consequently, digital marketing has developed into a balancing act between personalised address and overstepping the 'creepy line'. As if this were not enough, the need for legally-compliant conduct has been additionally attracting attention since the GDPR came into force. After all, both commercial businesses and their affiliated service providers as contracted data processors are liable in the event of data protection breaches. Today, this cornucopia of growing and ever-changing requirements determines the everyday lives of those working in marketing. All the more reason to provide them with highly-functional e-mail marketing automation that decisively reduces the work involved through future-oriented marketing features, automation and legal compliance.

In the following article, Andres Dickehut – CEO of IT and marketing services provider Consultix – explains why his ProCampaign digital marketing platform addresses precisely this and efficiently supports marketing professionals in planning and executing campaigns. Dickehut and his team included all aspects of data protection and IT security in the product's development from the very outset. For this reason, the digital marketing cloud offers numerous functions that provide marketing managers with practical tools and hence the security to fulfil the requirements of the GDPR.

In dialogue marketing, the legal position relating to the consent for processing personal data – so-called "permission management" – is relevant: the GDPR furnishes consumers whose data are collated, saved and processed with further rights. Concretely, the requirements relating to consent, among other things, are becoming tighter. Consent must be provided by persons capable of doing so, voluntarily for the concrete case and unmistakably in an informed manner in the form of a declaration or other unambiguous action. One core issue here is the tying prohibition, which specifies that companies are no longer permitted to tie a service to the consent to process data if this is not necessary for the fulfilment of the purpose. For example, online shops are not permitted to tie the delivery of goods to a consent relating to tracking, targeting or the personalisation of further advertising. In terms of operations, this means that consent is provided actively – ideally via the familiar double opt-in procedure. To be able to verify that this consent has actually been provided, the texts must be saved in a secure and compliant manner. Here, the latest version of ProCampaign offers the 'Permission Text Management' module and hence compliant management of all permission and legal texts. Thanks to this module, the hub stores the temporary versions of the consent for each customer profile provided by the customer.

Furthermore, the GDPR principle of data minimisation is also of tremendous importance to marketing departments: according to this, companies are now only permitted to request and save customer data that are "appropriate and relevant to the purpose". Consequently, marketers must analyse what customer data they actually require and what data they are no longer permitted to save and must therefore delete. In detail, they must ensure that only those data fields required for providing the service are included as mandatory fields in all forms requesting data.

For example, ProCampaign's response to this is automated clean-up processes that take all legal requirements into account. Users can be certain that the cleansing process automatically deletes all data that may no longer be saved. Furthermore, the system is able to demand that all other 'docked' systems also delete the respective person's data – a considerable workload reduction for marketing managers who use more than one tool in their day-to-day work. With regard to personal rights, person-related data must in future be saved in a transparent manner and those affected comprehensively informed about how their data are being used. Here, data storage should ideally be in Germany or – if not – in the EU. Customer data from the ProCampaign hub are stored securely in a company-owned high-security Data Center in Germany. In terms of transparency, the tool works with change logs. These logs capture all data changes in the system, ensuring that it is possible to subsequently track who changed what data. However, there are – even under these prerequisites – stipulations that marketers have to adhere to. For instance, users must also regularly delete all change logs to prevent data that may no longer be saved from still being present on systems. If a customer insists on their right to have their data deleted and to 'be forgotten', ProCampaign will also automatically inform 'docked' systems that a customer has requested that their data be deleted.

A further requirement of the GDPR is to provide – on request – consumers with all their saved personal data within 30 days. This is frequently not that simple in practice due to the fact that personal data are stored in silos and on various systems. Marketing managers can only quickly and comprehensively comply with this duty of disclosure if the overall set-up permits personal profile data to be exported at the press of a button and provide the consumer with these data as a bundle. For this, ProCampaign offers a fully-automatic process that enables simple extraction of all personal data saved – also from 'docked' systems. The software exports these data in a machine-readable file format, i.e. as a CSV file, so as to subsequently transfer the data to other systems in a simple and secure manner. Customers can initiate data exports in the login area, while internal staff and also employees can do so via the connected call centre. The process is useful when customers want to switch their medical insurance or mobile provider, for instance. This function allows companies to simply comply with the duty of disclosure in accordance with the GDPR.

Within the context of Consultix Professional Services, marketing managers benefit from the fact that all procedures and processes created while executing campaigns with ProCampaign are documented. So, all marketing professionals utilising the services acquire detailed campaign documentation and can – at all times and without any additional costs – explain where and how personal data has been collated and saved within the context of a campaign.

ANDRES DICKEHUT

Andres Dickehut is CEO of Consultix GmbH. The company's flagship product is ProCampaign®, the secure customer engagement hub. The marketing automation solution is EuroPriSe-certified and fully complies with the EU GDPR.

Consultix GmbH
info@consultix.net
procampaign.de

THE GROUP OF ANALYSTS