Can Suppression Lists be Used in a GDPR-Compliant Manner in Email Marketing? *

I. The Problem

It is standard practice for Email Service Providers (ESPs) to maintain client-specific or even global suppression lists (do-not-contact lists), in order to prevent the importation into the system of email addresses for which contact must under no circumstances be re-established. This may be because the recipient has complained in the past and has made the desire not to receive further emails from this sender explicit. An accidental re-import of the affected address would not only anger the recipient, but would also damage the reputation of the sender. Saving the email address despite a withdrawal of consent or a request for deletion may well infringe the data protection provisions. However, if the affected email address is removed from a suppression list, there is the danger that the recipient might be contacted again.

II. Possible Technical Procedures for the Creation of a Suppression List

A first, simple approach (Variant 1)

Instead of saving the email address in plain text, a so-called hash value is simply saved in the suppression list. If a corresponding hash algorithm is used for the generation of hash values, the re-establishment of the email address on the basis of the hash value is not readily possible. When new addresses are imported into the system, a hash value must be generated for each of them using the same algorithm. This value is then compared with the values on the suppression list. If there is a match, it is clear that the associated address is blocked and is not to be re-imported.

Problems with Variant 1

Variant 1 has two significant weaknesses. The first is that hash algorithms "age". This means that a hash algorithm that is considered secure today will under certain circumstances in future, as a result of technical developments, no longer be irreversible, and thus the original email addresses could be reconstructed from the existing hash values. The well-known hash algorithm Message-Digest Algorithm 5 (MD5), for example, which was developed in 1991, is no longer considered secure.

In addition to this, there is the problem of so-called Rainbow Tables. On principle, a hash algorithm must deliver the same result for the same input. With a manageable input of

time and resources, this can potentially be exploited to – simply put – create a very large table in which all possible input values are entered, and the associated hash values are calculated. Hash values can then be looked up in this table, and thus the original email address can be reconstructed.

Improvement form a technical perspective (Variant 2)

The problems of this first approach can, however, be averted. The "aging" of the algorithm cannot be prevented. However, it is possible to "rehash" hash values that were generated with an algorithm that is no longer considered secure with a new, modern and secure algorithm. The old hash value thus becomes the input for the new algorithm. After this step has been taken, the old hash values can be deleted.
Nevertheless, the "recipe" with which the latest hash values on the suppression list were generated must also be documented, so that it remains possible to cross-check addresses against the suppression list.

The problem with Rainbow Tables can be circumvented through "salt". A salt is ideally a random value that is attached to the actual value – e.g. the email address – before the hash value is calculated. The salt does not need to be kept secret to be effective, and can be stored together with the hash value and the "recipe" in the suppression list. For this Variant 2, it would also be theoretically possible to create a separate Rainbow Table for every potential salt. In this case, instead of just one very big table, one would need to create a huge number of such tables. But this would require such a massive input of time and resources that it would no longer be a practicable approach.

III. Legal Assessment of the Approaches Presented

In the context of the following legal examination it is to be assessed to what extent the two technical procedures presented above are compatible with the EU-GDPR. To achieve this, it must first be clarified to what extent suppression lists contain personal data, given that the GDPR is only then applicable.

Personal Data

The field of application of the GDPR is opened when personal data is processed. Personal Data as a term is defined in Art. 4 Para. 1 (1) GDPR.[1] According to this definition, this includes all information that relates to an identified or identifiable natural person. The data subjects are identifiable if they can be directly or indirectly identified, especially by means of the attribution to an identifier such as a name, an ID number, locational data, an online identifier, or one or more special features that are an expression of the physical, physiological, genetic, psychological, economic, cultural, or social identity of this natural person. In practice, this includes all data that is or can in any way be attributed to a person.

Email addresses count as personal data.[2] What is open to question is whether the provisions of the GDPR are applicable for the use of hash values standing for email addresses. For the regulation to be applicable, the hash values would also need to be considered personal data. What is decisive at this point is whether the use of hash algorithms represents pseudonymization or anonymization.

Defining Pseudonymization and Anonymization

To fulfill the requirements of pseudonymization, it is sufficient to make changes to the dataset that impede the attribution to a natural person, if additional information and knowledge is needed to restore the attribution. This is regardless of whether the additional knowledge is actually made use of or not. The requirements for anonymization, rather than pseudonymization, would only be satisfied when obtaining the additional knowledge would require a disproportionate expenditure of time, money, and personnel resources. [3] Personal data that has undergone pseudonymization is considered information about an identifiable natural person.

In the case of anonymization, data minimization over and above pseudonymization is undertaken, so that it is either absolutely no longer possible to make a personal attribution or is only possible with disproportionate effort (see above). The processing of effectively anonymized datasets is not restricted by data protection law.

[1] Articles without more specific designations are those of the GDPR
[2] https://www.ldi.nrw.de/mainmenu_Datenschutz/Inhalt/FAQ/PersonenbezogeneDaten.php
[3] Däuble/ Wedde/ Weichert/ Sommer. EU-Datenschutz-Grundverordnung und BDSG-neu DSGVO Artikel 4 Rdnr. 76

Personal Data in Variant 1

Through the use of hash algorithms as defined for Variant 1, as described above, the attribution to a specific person is somewhat impeded, but remains possible without a great deal of effort. This variant represents a pseudonymization of personal data, which is subject to data protection stipulations.

Personal Data in Variant 2

As can be seen above, the attribution of the email address in question would only be possible at a very considerable input in terms of time and work with normally available tools. Even for state institutions, which have further possibilities at their disposal, ascertaining the email address behind the hash value would, if at all, only be possible under difficult conditions. The process should no longer be defined under the data protection legal term of pseudonymization. Rather, it is to be deemed anonymization.

Interim Result

Through the use of Variant 1, the danger exists that the attribution to the data subject remains possible without a great deal of effort, with the consequence that the process would be considered pseudonymization. The data protection regulations must therefore be observed. The GDPR is thus applicable.

The legal situation is to be assessed differently for the use of that hash method as described in Variant 2. As a result of the unreasonable amount of effort that would be required for the allocation of data to the data subject, this is to be considered anonymization. Therefore, there are no personal data contained within Variant 2. The use is thus in principle quite safe from the perspective of data protection law.

Compatibility of Variant 1 with the GDPR

If companies only have the possibility of using Variant 1, the question arises as to whether this procedure is possible at all according to data protection law. According to Article 6 Para. 1 GDPR, the processing of personal data is only permissible either with the consent of the data subject or in the presence of one of the defined exceptions which make it permissible.

Essentially, what comes under consideration here is the presence of a consent declaration according to Article 6 Para. 1 (a) and the exemption given in Article 6 Para.1 (f), which

allows the processing in the case of a legitimate interest of the data processor, when this is not overridden by the interests of the data subject requiring special protection.

a) Consent according to Art. 6 Para. 1 (a)

The processing of personal data of a data subject for one or more purposes is, according to Art. 6 Para. 1 (a) legal when the data subject has given consent. A declaration of consent for a specific case must be voluntarily granted in an informed manner, and must fulfill the general requirements given in Art. 7.[4]

Companies that wish to implement Variant 1 legally would therefore need to obtain a formal legal declaration of consent from the data subject. Consequently, the data controller would need to approach every person individually and request consent for the processing of the email address for the purposes of establishing a suppression list. Further to this, every declaration of consent would need to be documented for the purpose of securing evidence. Even if the declaration of consent were to prove to be the most legally certain means, the obtaining of this would for most companies not be very practicable, especially not in the case where the consent would need to be obtained at a later date for every single data subject.

One approach to consider would be to obtain the consent for the use of the email address for the establishment of a suppression list at the same time as the consent for the sending of marketing emails. In this case, it is essential that the formal requirements in Art. 7 GDPR are observed, and two separate consent declarations are formulated. In addition to this, the data subject can also withdraw consent for the use of his/her data for the purpose of establishing a suppression list, according to Art. 7 Para. 3.

b) Legitimate interest according to Art. 6 Para. 1 (f)

The stipulation in Art. 6 Para. 1 (f) permits the processing of personal data when this is necessary to protect the legitimate interests of the data controller or third parties. The permissibility of processing on the basis of this exception is subject to the proviso that the data subject has no overriding interests or fundamental rights or freedoms that demand the protection of personal data. The required balancing of interests is the responsibility

[4] Däuble/ Wedde/ Weichert/ Sommer. EU-Datenschutz-Grundverordnung und BDSG-neu DSGVO Artikel 6 Rdnr. 16

of the data controller.[5] The interests of the data subject relate to the protection of his/her own personal data.

If the data subject has withdrawn consent for the use of his/her personal data for the purposes of being addressed by marketing material by email, justification for the processing of this data in a suppression list could nonetheless be affirmed. Through the establishment of a suppression list, the data controller wishes to ensure that email addresses for which consent for their use for marketing purposes has been withdrawn cannot be reused for this purpose. The re-use of the data subject's email address for marketing purposes – whether deliberate or accidental – can in this way be prevented. Through pseudonymization, the data are also in principle protected against unauthorized access by third parties, and therefore the risk of attribution reduces.

Given that this procedure supports the interests of the data subject, it is highly probable that the legitimate interest of the data controller will be affirmed. The question arises as to what the legal situation is in the event that the data subject requests deletion.

According to Article 17 GDPR, the data subject can demand the deletion of his/her personal data and the data controller must delete the affected data without delay, insofar as one of the grounds in Art. 17 Para. 1 (a-f) applies and there is no exception as defined in Art. 17 Para. 3.

What could be interesting in Art. 17 Para. 1 (b and c): According to these, the email address of the data subject is to be deleted when a withdrawal of consent or an objection exists and no further legal grounds exist for the processing.
As further legal grounds, the legitimate interest of the data controller as defined in Art. 6 Para. 1 (f) again comes under consideration.
In this respect, the argumentation of legitimate interest can be referenced.

IV. Summary and Recommendations:

The use of Variant 1 is generally problematic. Given that the attribution to the person behind the email address is possible without disproportionate effort, the requirements of data protection law must be observed. It is conceivable to process data legitimately through the balancing of the respective interests, but this does not offer 100-percent legal certainty. The declaration of consent offers greater legal certainty: However, the

[5] Däuble/ Wedde/ Weichert/ Sommer. EU-Datenschutz-Grundverordnung und BDSG-neu DSGVO Artikel 6 Rdnr. 90 ff.

obtaining of prior consent would definitely require the fulfillment of the strict formal requirements of the GDPR.

Consequently, Variant 2 is therefore preferable. Given that an attribution of the email address to the data subject is only possible with disproportionate means, this legal examination takes the opinion that this procedure is one of anonymization, which is not included in the field of application of data protection law.

Status: November 2018

** Legal Disclaimer: This article makes no claim to legal certainty or exhaustiveness. Its purpose is to point out the possible problems.*

Authors: Alexander Zeh, Engineering Manager
and Rosa Hafezi, Legal Counsel
Certified Senders Alliance